



governmentattic.org

"Rummaging in the government's attic"

Description of document: Securities and Exchange Commission (SEC) Office of Inspector General (OIG) Findings and Recommendations, 2005 (Federal Information Security Management Act) FISMA Assessment for the EFOIA Application

Requested date: 19-August-2017

Release date: 09-January-2018

Posted date: 31-December-2018

Source of document: Freedom of Information Act Request
Freedom of Information Act Officer
SEC
100 F Street NE
Washington, DC 20549
Fax: 202-772-9337
Email: foiapa@sec.gov
[Online Request for Copies of Documents form](#)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
STATION PLACE
100 F STREET, NE
WASHINGTON, DC 20549-2465

Office of FOIA Services

January 9, 2018

Re: Freedom of Information Act (FOIA), 5 U.S.C. § 552
Request No. 17-00090-OIG

This letter is in response to your request dated August 19, 2017, and received in this office on August 28, 2017, for a copy of the nonpublic technical report associated with Audit Number 410, dated 2005.

The search for responsive records has resulted in the retrieval of 78 pages of records that may be responsive to your request. They are being provided to you with this letter, except for certain portions that are being withheld pursuant to 5 U.S.C. § 552(b)(7)(E), 17 CFR § 200.80(b)(7)(v). Exemption 7(E) protects information compiled for law enforcement purposes if disclosure would reveal specific investigative techniques, guidelines, or procedures, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

I am the deciding official with regard to this adverse determination. You have the right to appeal my decision to the SEC's General Counsel under 5 U.S.C. § 552(a)(6), 17 CFR § 200.80(d)(5)(iv). The appeal must be received within ninety (90) calendar days of the date of this adverse decision. Your appeal must be in writing, clearly marked "Freedom of Information Act Appeal," and should identify the requested records. The appeal may include facts and authorities you consider appropriate.

You may file your appeal by completing the online Appeal form located at https://www.sec.gov/forms/request_appeal, or mail your appeal to the Office of FOIA Services of the Securities and

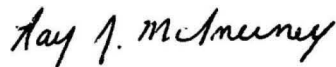
January 9, 2018
Page 2

Exchange Commission located at Station Place, 100 F Street NE, Mail Stop 2465, Washington, D.C. 20549, or deliver it to Room 1120 at that address. Also, send a copy to the SEC Office of the General Counsel, Mail Stop 9612, or deliver it to Room 1120 at the Station Place address.

You also have the right to seek assistance from me as a FOIA Public Liaison or contact the Office of Government Information Services (OGIS) for dispute resolution services. OGIS can be reached at 1-877-684-6448 or Archives.gov or via e-mail at ogis@nara.gov.

If you have any questions, please contact Sonja L. Osborne of my staff at osbornes@sec.gov or (202) 551-8371. You may also contact me at foiapa@sec.gov or (202) 551-7900.

Sincerely,

A handwritten signature in black ink that reads "Ray J. McInerney". The signature is written in a cursive, slightly slanted style.

Ray J. McInerney
FOIA Branch Chief

Enclosure

Findings and Recommendations

2005 FISMA Assessment for the EFOIA Application
Assigned Task 8



U.S. Securities and Exchange Commission
Office of Inspector General

Submitted to
Mr. Nelson Egbert
Deputy Inspector General

September 9, 2005

From



2750 Prosperity Avenue, Suite 510
Fairfax, Virginia 22031

Contact Person
Bob Richardson
Project Manager
Phone (703) 270-1540 Fax (703) 270-1541



Table of Contents

EXECUTIVE SUMMARY	1
1 INTRODUCTION	3
1.1 Evaluation Objectives	3
1.2 Scope	4
1.3 Methodology and Process Description	5
1.4 Documentation Review	5
1.5 Staff Interviews	6
1.6 Visual Inspections	6
2 EVALUATION RESULTS	8
2.1 System Environment	8
2.2 Findings.....	9
(b)(7)(E)	10
	11
	12
	12
	13
	14
	14
APPENDIX A FISMA CHECKLIST FOR EFOIA	16
A.1 Management Controls	16
A.2 Operational Controls	27
A.3 Technical Controls.....	56

SEC CONFIDENTIAL



Executive Summary

ECS recently performed an assessment of one of the SEC's major applications (EFOIA) as required by the Federal Information Security Management Act (FISMA). The goal of this evaluation was to help the OIG perform an independent evaluation of the EFOIA application in order to meet its responsibilities under FISMA.

The findings in this report are categorized by levels of risk and identify the resulting security vulnerabilities. Significant deficiencies are high- or medium-risk vulnerabilities. High-risk vulnerabilities pose an immediate threat to the security of the system or its data and should be addressed immediately. Medium-risk vulnerabilities are issues that must be addressed in a timely manner (e.g., the next 3 to 6 months) and have the potential for the same ramifications associated with the high risk category. Low vulnerabilities are issues that do not pose an immediate or critical threat, but must be addressed at a later date.

During this evaluation, ECS found (b)(7)(E)

(b)(7)(E)

SEC CONFIDENTIAL



In order to mitigate these weaknesses, ECS recommends that the SEC consider implementing the following:

(b)(7)(E)

SEC CONFIDENTIAL

1 Introduction

The U.S. Securities and Exchange Commission (SEC), Office of Inspector General (OIG), contracted with Electronic Consulting Services, Inc. (ECS) to perform an assessment of two of the SEC's major applications as required by the Federal Information Security Management Act (FISMA). The applications chosen by the SEC were ACTS Plus and EFOIA. This included an evaluation of the SEC's information security policies, practices, and procedures as it relates to the applications. A report on the results of the evaluation will accompany the Chairman's 2005 budget submission to the Office of Management and Budget (OMB). This document describes the FISMA evaluation results of the EFOIA application. The results of the ACTS Plus evaluation are presented in the report *Findings and Recommendations: 2005 FISMA Assessment for the ACTS Plus Application*.

1.1 Evaluation Objectives

The objectives of this evaluation were threefold: 1) Perform the necessary evaluation procedures to answer those questions published by OMB in its reporting guidance; 2) Compile an Executive Summary for the SEC's OIG; and 3) Perform an assessment of two of the SEC's major systems that have been certified and accredited (ACTS Plus and EFOIA).

The 2005 independent FISMA evaluation and accompanying OIG Executive Summary will answer OMB's 2005 questions on the Commission's information security program. The 2005 OMB guidance is similar to prior year guidance in requiring the OIG to independently evaluate and report on how the Chairman, Chief Information Officer, and program officials implemented mandated information security requirements related to information systems program reviews; life cycle security; security incident and response; corrective action reporting; and measuring information security performance.

To accomplish these objectives, ECS:

- Obtained and reviewed pertinent SEC documents, policies, and procedures and compared them with the applicable Federal standards
- Conducted interviews with pertinent staff at the operations center (OPC) in Alexandria, VA, to assess staff knowledge and implementation of SEC IT security policies and procedures
- Evaluated and observed the physical controls implemented according to the applications' system security plan (SSP)
- Provided updates on the findings to SEC Management and the OIG
- Submitted the assessment results in an Executive Summary as well as more detailed Findings and Recommendations

SEC CONFIDENTIAL



1.2 Scope

The scope of the evaluation for this report was EFOIA, which is a major application that is owned by the SEC's Office of Filing and Information Services (OFIS). The EFOIA major application is actually a COTS application called FOIAXpress by AINS Inc. The SEC has configured the FOIAXpress application to meet its business goals. Those configuration changes as well as the security of the COTS portions of the application are included in the scope of the assessment.

ECS performed an assessment of the application as required by the Computer Security Act of 1987 to determine if the application meets the necessary security requirements prescribed in the Federal Information Systems Control Audit Manual (FISCAM) and National Institute of Standards and Technology (NIST) Special Publications 800-53. Components of the SEC's Security Program that were evaluated included:

- SEC's security management structure
- Risk management process
- System security plans
- Certification and accreditation process
- Computer incident response capability
- Contingency planning process and procedures
- Security awareness environment
- Life-cycle management of security, management of personnel security
- Privacy

ECS reviewed the SEC's Plan of Actions and Milestones (POA&Ms) for the application and assessed its progress and process for tracking and correcting reported security weaknesses. ECS also performed an evaluation to answer the questions published by OMB in its reporting guidance and will compile an Executive Summary for the SEC OIG that summarizes the answers to the questions. ECS will determine whether the conclusions reached during the OIG Independent Evaluation are consistent with the conclusions reported in the SEC Management self-evaluation of the SEC's Information Security Program.

ECS performed an information security assessment of EFOIA that addressed:

- Adequacy, strengths, and weaknesses related to physical security
- User identification and authentication
- Logical access controls

SEC CONFIDENTIAL



- Detective controls, such as audit trails, hardware, and systems maintenance
- Production input/output controls
- Data integrity

ECS will recommend improvements to the SEC's management controls and privacy policies as appropriate. The evaluation was performed in accordance with Government Auditing Standards 2003 (the Yellow Book).

1.3 Methodology and Process Description

To determine whether the IT security objectives have been met, ECS used the following methods and processes:

- Documentation Review – When applicable, a review of the requirements contained in the SEC's IT regulations was performed to determine the SEC's level of compliance as well as the policies' effectiveness.
- Staff Interviews – Discussions with SEC personnel within OFIS were conducted to identify personnel knowledge level as well as risks, vulnerabilities, and/or threats that exist in the current operating environment that they are aware of or concerned about or that are caused by insufficient security controls, policies, and procedures.
- Visual Inspections – Visual inspections were performed to ensure that physical and electronic data and IT systems were adequately protected.

1.4 Documentation Review

ECS reviewed the following standards, system, and security documents:

- EFOIA Security Documentation:
 - EFOIA Application Risk Assessment Report
 - System Security Plan (SSP) for the EFOIA Application
 - ST&E Results Report for the EFOIA Application
 - Plan of Action and Milestones (POA&Ms) for EFOIA
 - Disaster Recovery Plan (DRP) for the EFOIA Major Application
- EFOIA System Documentation:
 - Standard Operating Procedures for FOIAXpress V5.2.7
 - FX and SX Production Server Scenario
- Applicable IT Security Laws and Standards:
 - SEC regulations, such as the IT Rules of the Road
 - Federal Information Security Management Act (FISMA) of 2002
 - Office of Management and Budget (OMB) Circular A-130

SEC CONFIDENTIAL

- Computer Security Enhancement Act of 1997
- The Privacy Act
- Homeland Security Presidential Directive/Hspd-7
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-18, Guide for Developing Security Plans for IT Systems
- NIST SP 800-30, Risk Management Guide for IT Systems
- NIST SP 800-34, Contingency Planning Guide for IT Systems
- NIST SP 800-47, Security Guide for Interconnecting IT Systems
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems

1.5 Staff Interviews

ECS interviews are intended to help identify:

- Important application and data security issues
- Customers, partners, and vendors that affect the security of the application
- Application hosting, monitoring, and reporting tasks
- Events that require response and escalation procedures
- Incident detection and diagnostic tools and procedures

Because EFOIA is a COTS product that does not require programming or customization, knowledgeable staff was limited; therefore, ECS only interviewed the EFOIA system owner. The system owner was able to answer all of the questions based on NIST SP 800-53 pertaining to the management, operational, and technical controls of the system.

In addition, the EFOIA servers and communication equipment are maintained by OIT in the SEC's data center. ECS understands that the data center is currently undergoing an evaluation by GAO as part of the FISMA review of the General Infrastructure Support System (GSS). Therefore, to avoid duplication of work, ECS did not generally include OIT or data center members in its interview process for EFOIA, except where needed for application issues.

1.6 Visual Inspections

ECS verified physical security and asset management by visually inspecting OFIS facilities to ensure that critical data is protected at all times. This included inspections and

SEC CONFIDENTIAL



walkthroughs of office spaces, entry locks, and card key access mechanisms on the second floor that that FOIA/PA Branch of OFIS occupies in the Operations Center (OPC) at 6432 General Green Way in Alexandria, VA.

SEC CONFIDENTIAL

2 Evaluation Results

EFOIA is a major application used by the Office of Filing and Information Services (OFIS) to process Freedom of Information Act (FOIA) and Privacy Act (PA) requests from individuals and businesses. The application is actually a commercial-off-the-shelf (COTS) product called FOIAXpress developed by AINS, Inc. FOIAXpress is used by several U.S. Government agencies in addition to the SEC.

FOIAXpress is a web-based application that provides for efficient FOIA/PA/Appeal request processing. FOIAXpress electronically creates, stores, retrieves, redacts, and prints documents for delivery to FOIA requesters. It also keeps track of FOIA processing statistics and fees in addition to generating reports on the number, types, and nature of FOIA requests processed, as required by the U.S. Department of Justice

The SEC uses FOIAXpress (EFOIA) to receive, process, and disclose FOIA and Privacy Act (PA) records. EFOIA does not generate new information; whenever OFIS needs records or additional information to respond to public requests, it contacts other SEC offices to obtain these records, especially those stored in SEC applications or databases like the Name Relationship Search Index (NRSI) application and the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. Most processes within EFOIA are automated.

2.1 System Environment

EFOIA	(b)(7)(E)
(b)(7)(E)	

SEC CONFIDENTIAL

2.2 Findings

Even though EFOIA is not considered a critical application for the SEC, it has a risk rating of (b)(7)(E)

(b)(7)(E) The risk level influences the agency's selection of security controls to protect the system.

ECS performed the FISMA evaluation in accordance with NIST SP800-53, which provides a comprehensive list of security controls for federal information systems. Using 800-53 as a guide, and assessing the controls specified for systems categorized as (b)(7)(E) in FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, during this evaluation, ECS identified (b)(7)(E)

(b)(7)(E)

A *significant finding* is defined as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. Significant deficiencies are usually high- or medium-risk vulnerabilities. A *reportable condition* is a low-risk vulnerability that does not have to be fixed immediately, but be addressed at some time in the future.

Agencies are no longer required to report the number of significant deficiencies during the annual FISMA report to OMB; however, all security weaknesses must be included in and tracked on the system's POA&Ms.

The EFOIA findings are described in more detail in the subsections below.

SEC CONFIDENTIAL

2.2.1

(b)(7)(E)

A C&A was performed in (b)(7)(E)

(b)(7)(E)

Recommendation A

(b)(7)(E)

SEC CONFIDENTIAL



(b)(7)(E)

Response from OIT

Refer to the document *Response to Draft Report from SEC OIG, 9/12/05*, written by OIT and SAIC (the contractor who performed the C&A for EFOIA).

Evaluation of OIT's Response

Refer to the document *Response to Draft Report from SEC OIG, 9/12/05*, written by OIT and SAIC (the contractor who performed the C&A for EFOIA).

2.2.2

(b)(7)(E)

Recommendation B

(b)(7)(E)

Response from OIT

(b)(7)(E)

Evaluation of OIT's Response

(b)(7)(E)

SEC CONFIDENTIAL

(b)(7)(E)

2.2.3

2.2.4

SEC CONFIDENTIAL

(b)(7)(E)

2.2.5

Response from OFIS

The FOIA Office will incorporate these existing procedures into the internal Administrative Manual.

Evaluation of OFIS's Response

ECS agrees with OFIS's plan to document these procedures.

SEC CONFIDENTIAL

2.2.6

(b)(7)(E)

2.2.7

SEC CONFIDENTIAL



(b)(7)(E)

SEC CONFIDENTIAL



Appendix A FISMA Checklist for EFOIA

A.1 Management Controls

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. The results of ECS's evaluation of EFOIA's management controls are shown in the last two columns of this control table. These results indicate whether the control was met or not (Yes/No/Partial) and why (Auditor's Comments).

Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
RA-1	Risk Assessment Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls	The risk assessment policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures.	(b)(7)(E)	
RA-2	Security Categorization	Verify that the organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Verify that designated senior-level officials within the organization review and approve the security categorizations.	NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. The organization conducts security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
RA-3	Risk Assessment	Verify that the organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.	<p>Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system.</p> <p>NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.</p>	(b)(7)(E)	
RA-4	Risk Assessment Update	Verify that the organization updates the risk assessment regularly or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.	<p>The organization develops and documents specific criteria for what is considered significant change to the information system.</p> <p>NIST Special Publication 800-30 provides guidance on conducting risk assessment updates.</p>		
RA-5	VULNERABILITY SCANNING	Verify that, using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system regularly or when significant new vulnerabilities affecting the system are identified and reported.	<p>The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques.</p> <p>The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.</p> <p>Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code).</p> <p>NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 provides guidance on handling security patches.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PL-1	Security Planning Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls	The security planning policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security planning policy can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.	(b)(7)(E)	
PL-2	System Security Plan	Verify that the organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	NIST Special Publication 800-18 provides guidance on security planning.		
PL-3	System Security Plan Update	Verify that the organization reviews the security plan for the information system regularly and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	Significant changes are defined in advance by the organization and identified in the configuration management process.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PL-4	Rules of Behavior	<p>Verify that the organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage.</p> <p>The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system.</p>	<p>Electronic signatures are acceptable for use in acknowledging rules of behavior.</p> <p>NIST Special Publication 800-18 provides guidance on preparing rules of behavior.</p>	(b)(7)(E)	
PL-5	Privacy Impact Assessment	Verify that the organization conducts a privacy impact assessment on the information system.	OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Gov Act of 2002.		
SA-1	System and Services Acquisition Policy and Procedures (b)(7)(E)	<p>Verify that the organization develops, disseminates, and periodically reviews/updates:</p> <p>(i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance</p> <p>(ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls</p>	<p>The system and services acquisition policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.</p> <p>The system and services acquisition policy can be included as part of the general information security policy for the organization.</p> <p>System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required.</p> <p>NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SA-2	Allocation of Resources	Verify that the organization determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information system.	<p>The organization includes the determination of security requirements for the system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation.</p> <p>NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process.</p>	(b)(7)(E)	
SA-3	Life Cycle Support	Verify that the organization manages the information system using a system development life cycle methodology that includes information security considerations.	NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.		
SA-4	Acquisitions	Verify that the organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.	<p>The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe:</p> <ul style="list-style-type: none">(i) required security capabilities(ii) required design and development processes(iii) required test and evaluation procedures(iv) required documentation <p>The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.</p> <p>Refer to NIST Special Publications 800-53, 800-36, 800-35, 800-64, 800-23, and 800-70.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SA-5	Information System Documentation	Verify that the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.	Administrator and user guides include information on: (i) configuring, installing, and operating the information system (ii) optimizing the system's security features NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.	(b)(7)(E)	
SA-6	Software Usage Restrictions (b)(7)(E)	Verify that the organization complies with software usage restrictions.	Software and associated documentation is used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		
SA-7	User Installed Software (b)(7)(E)	Verify that the organization enforces explicit rules governing the downloading and installation of software by users.	If provided the necessary privileges, users have the ability to download and install software. The organization identifies what types of software downloads and installations are permitted (e.g., updates and security patches to existing software) and what types of downloads and installations are prohibited (e.g., software that is free only for personal, not government, use). The organization also restricts the use of install-on-demand software.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SA-8	Security Design Principles	Verify that the organization designs and implements the information system using security engineering principles.	NIST Special Publication 800-27 provides guidance on engineering principles for information system security.	(b)(7)(E)	
SA-9	Outsourced Information System Services	Verify that the organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.	Third-party providers are subject to the same information system security policies and procedures of the supported organization, and must conform to the same security control and documentation requirements as would apply to the organization's internal systems. Appropriate organizational officials approve outsourcing of information system services to third-party providers (e.g., service bureaus, contractors, and other external orgs). The outsourced information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service level agreements. Service level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on the security considerations in the system development life cycle.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SA-10	DEVELOPER CONFIG MGMT (b)(7)(E)	Verify that the information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.		(b)(7)(E)	
SA-11	DEVELOPER SECURITY TESTING (b)(7)(E)	Verify that the information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.	Developmental security test results should only be used when no security relevant modifications of the information system have been made subsequent to developer testing and after selective verification of developer test results.		
CA-1	Certification, Accreditation, and Security Assessment Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.	The security assessment and certification and accreditation policies and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on processing security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
CA-2	Security Assessment	Verify that the organization conducts an assessment of the security controls in the information system at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	<p>This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be tested with a frequency depending on risk, but no less than annually.</p> <p>NIST Special Publications 800-53A and 800-26 provide guidance on security control assessments.</p>	(b)(7)(E)	
CA-3	Information System Connections	Verify that the organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.	<p>Since FIPS 199 security categorizations apply to individual information systems, the organization should carefully consider the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations should also include information systems sharing the same networks.</p> <p>NIST Special Publication 800-47 provides guidance on interconnecting information systems.</p>		
CA-4	Security Certification	Verify that the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	<p>A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system.</p> <p>The security certification is integrated into and spans the System Development Life Cycle (SDLC).</p> <p>NIST Special Publication 800-53A provides guidance on the assessment of security controls. NIST Special Publication 800-37 provides guidance on security certification and accreditation.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
CA-5	Plan of Action and Milestones	Verify that the organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	<p>The plan of action and milestones (POA&M) updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.</p> <p>The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official.</p> <p>NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. NIST Special Publication 800-30 provides guidance on risk mitigation.</p>	(b)(7)(E)	
CA-6	Security Accreditation	<p>Verify that the organization authorizes (i.e., accredits) the information system for processing before operations and <i>updates the authorization</i> after major changes.</p> <p>A senior organizational official signs and approves the security accreditation.</p>	<p>OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems.</p> <p>The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications.</p> <p>NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
CA-7	Continuous Monitoring	Verify that the organization monitors the security controls in the information system on an ongoing basis.	<p>Continuous monitoring activities include:</p> <ol style="list-style-type: none">1. Configuration management and control of information system components2. Security impact analyses of changes to the system3. Ongoing assessment of security controls4. Status reporting <p>The organization establishes the selection criteria for control monitoring and subsequently selects a subset of the security controls employed within the information system for purposes of continuous monitoring.</p> <p>NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls.</p>	(b)(7)(E)	

SEC CONFIDENTIAL



A.2 Operational Controls

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. The results of ECS's evaluation of EFOIA's operational controls are shown in the last two columns of this control table. These results indicate whether the control was met or not (Yes/No/Partial) and why (Auditor's Comments).

Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PS-1	Personnel Security Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	The personnel security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	(b)(7)(E)	
PS-2	Position Categorization	Verify that the organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises risk designations as necessary.	Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PS-3	Personnel Screening	Verify that the organization screens individuals requiring access to organizational information and information systems before authorizing access.	Screening is consistent with: (i) 5 CFR 731.106(a) (ii) Office of Personnel Management policy, regulations, and guidance (iii) organizational policy, regulations, and guidance (iv) FIP S201 and Special Publications 800-73 and 800-76 (v) the criteria established for the risk designation of the assigned position	(b)(7)(E)	
PS-4	Personnel Termination	When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.			

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PS-5	Personnel Transfer	Verify that the organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).		(b)(7)(E)	
PS-6	Access Agreements	Verify that the organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access.			
PS-7	Third-Party Personnel Security	Verify that the organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.	The organization explicitly includes personnel security requirements in acquisition-related documents. NIST Special Publication 800-35 provides guidance on information technology security services.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PS-8	Personnel Sanctions [Enforcement]	Verify that the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	<p>The sanctions process is consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.</p> <p>The sanctions process can be included as part of the general personnel policies and procedures for the organization.</p>	(b)(7)(E)	
PE-1	Physical and Environmental Protection Policy and Procedures (b)(7)(E)	<p>Verify that the organization develops, disseminates, and periodically reviews/updates:</p> <p>(i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance</p> <p>(ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls</p>	<p>The physical and environmental protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.</p> <p>The physical and environmental protection policy can be included as part of the general information security policy for the organization.</p> <p>Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required.</p> <p>NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PE-2	Physical Access Authorizations	<p>Verify that the organization develops and keeps current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards).</p> <p>Designated officials within the organization review and approve the access list and authorization credentials at least annually.</p>	The organization promptly removes personnel no longer requiring access from access lists.	(b)(7)(E)	
PE-3	Physical Access Control	<p>Verify that the organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities.</p> <p>The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.</p>	<p>The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems.</p> <p>The organization secures keys, combinations, and other access devices and inventories those devices regularly.</p> <p>The organization changes combinations and keys:</p> <ul style="list-style-type: none"> (i) periodically (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated <p>After an emergency-related event, the organization restricts reentry to facilities to authorized individuals only.</p> <p>Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PE-4	Access Control for Transmission Medium	Verify that the organization controls physical access to information system transmission lines carrying unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering.	NOT SELECTED FOR BASELINE	(b)(7)(E)	
PE-5	Access Control for Display Medium	Verify that the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.			
PE-6	Monitoring Physical Access (b)(7)(E)	Verify that the organization monitors physical access to information systems to detect and respond to incidents.	The organization: 1. Reviews physical access logs periodically 2. Investigates apparent security violations or suspicious physical access activities 3. Takes remedial actions		
PE-7	Visitor Control	Verify that the organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.	Government contractors and others with permanent authorization credentials are not considered visitors.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PE-8	Access Logs	Verify that the organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting (ii) signature of the visitor (iii) form of identification (iv) date of access (v) time of entry and departure (vi) purpose of visit (vii) name and organization of person visited Designated officials within the organization review the access logs after closeout.		(b)(7)(E)	
PE-9	Power Equipment and Cabling	Verify that the organization protects power equipment and power cabling for the information system from damage and destruction.			

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PE-10	Emergency Shutoff	Verify that for specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization provides the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.		(b)(7)(E)	
PE-11	Emergency Power	Verify that the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.			
PE-12	Emergency Lighting	Verify that the organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.			
PE-13	Fire Protection	Verify that the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.	Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
PE-14	Temperature and Humidity Controls	Verify that the organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems.		(b)(7)(E)	
PE-15	Water Damage Protection	Verify that the organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.			
PE-16	Delivery and Removal	Verify that the organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.	The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized access. Appropriate organizational officials authorize the delivery or removal of information system-related items belonging to the organization.		
PE-17	Alternate Work Site [Remote access]	Verify that individuals within the organization employ appropriate information system security controls at alternate work sites.	NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications. The organization provides a means for employees to communicate with information system security staff in case of security problems.	(b)(7)(E)	

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
CP-1	Contingency Planning Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	The contingency planning policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.	(b)(7)(E)	
CP-2	Contingency Plan	Verify that the organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.			
CP-3	Contingency Training	Verify that the organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training at least annually.			

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
CP-4	Contingency Plan Testing	Verify that the organization tests the contingency plan for the information system at least annually using organization-defined tests and exercises to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.	There are several methods for testing contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises).	(b)(7)(E)	
CP-5	Contingency Plan Update	Verify that the organization reviews the contingency plan for the information system at least annually and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).		
CP-6	Alternate Storage Sites	Verify that the organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.			

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
CP-7	Alternate Processing Sites	Verify that the organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within a certain time period when the primary processing capabilities are unavailable.	Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site.	(b)(7)(E)	
CP-8	TELECOMMUNICATIONS SERVICES (b)(7)(E)	Verify that the organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within a certain time period when the primary telecommunications capabilities are unavailable.	In the event that the primary and/or alternate telecommunications services are provided by a wireline carrier, the organization should ensure that it requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).		
CP-9	Information System Backup	Verify that the organization conducts backups of user-level and system-level information (including system state information) contained in the information system at a certain frequency and stores backup information at an appropriately secured location.	The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
CP-10	Information System Recovery and Reconstitution	Verify that the organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.	Secure information system recovery and reconstitution to the system's original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available, and the system is fully tested.	(b)(7)(E)	
CM-1	Configuration Management Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the CM policy and associated configuration management controls	The CM policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The CM policy can be included as part of the general info security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.		
CM-2	Baseline Configuration	Verify that the organization develops, documents, and maintains a current, baseline configuration of the information system and an inventory of the system's constituent components.	The configuration of the information system is consistent with the Federal Enterprise Architecture and the organization's information system architecture. The inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
CM-3	Configuration Change Control	Verify that the organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.	Configuration change control involves the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes. The organization includes emergency changes in the configuration change control process.	(b)(7)(E)	
CM-4	Monitoring Configuration Changes	Verify that the organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.	The organization documents the installation of information system components. After the information system is changed, the organizations checks the security features to ensure the features are still functioning properly. The organization audits activities associated with configuration changes to the information system.		
CM-5	Access Restrictions for Change	Verify that the organization enforces access restrictions associated with changes to the information system.			
CM-6	Configuration Settings	Verify that the organization configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.	NIST Special Publication 800-70 provides guidance on configuration settings (i.e., checklists) for information technology products.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
CM-7	LEAST FUNCTIONALITY	Verify that the organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the certain functions, ports, protocols, and/or services.	<p>Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).</p> <p>The functions and services provided by information systems should be carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).</p>	(b)(7)(E)	
MA-1	System Maintenance Policy and Procedures (b)(7)(E)	<p>Verify that the organization develops, disseminates, and periodically reviews/updates:</p> <p>(i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance</p> <p>(ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls</p>	<p>The information system maintenance policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.</p> <p>The information system maintenance policy can be included as part of the general information security policy for the organization.</p> <p>System maintenance procedures can be developed for the security program in general, and for a particular information system, when required.</p> <p>NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>		
MA-2	Periodic Maintenance [Hardware]	Verify that the organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.	<p>Appropriate organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary.</p> <p>If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures.</p> <p>After maintenance is performed on the information system, the organization checks the security features to ensure that they are still functioning properly.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
MA-3	Maintenance Tools	Verify that the organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.		(b)(7)(E)	
MA-4	Remote Maintenance	Verify that the organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.	<p>The organization describes the use of remote diagnostic tools in the security plan for the information system.</p> <p>The organization maintains maintenance logs for all remote maintenance, diagnostic, and service activities. Appropriate organization officials periodically review maintenance logs.</p> <p>Other techniques to consider for improving the security of remote maintenance include:</p> <ul style="list-style-type: none">(i) encryption and decryption of diagnostic communications(ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special Publication 800-63(iii) remote disconnect verification		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
			<p>When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections. If password-based authentication is used during remote maintenance, the organization changes the passwords following each remote maintenance service.</p> <p>For high-impact information systems, if remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems before the connection of the remote access line.</p> <p>If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.</p>	(b)(7)(E)	
MA-5	Maintenance Personnel	<p>Verify that the organization maintains a list of personnel authorized to perform maintenance on the information system.</p> <p>Only authorized personnel perform maintenance on the information system.</p>	<p>Maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information.</p> <p>When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
MA-6	Timely Maintenance	Verify that the organization obtains maintenance support and spare parts for system components within a reasonable period of time after failure.		(b)(7)(E)	
SI-1	System and Information Integrity Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls	The system and information integrity policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SI-2	Flaw Remediation (Patch Management)	Verify that the organization identifies, reports, and corrects information system flaws.	<p>The organization identifies information systems containing proprietary or open source software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws).</p> <p>Proprietary software can be found in either commercial/government off-the-shelf information technology component products or in custom-developed applications.</p> <p>The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation.</p> <p>Flaws discovered during security assessments, continuous monitoring (see security controls CA-2, CA-4, or CA-7), or incident response activities (see security control IR-4) should also be addressed expeditiously.</p> <p>NIST Special Publication 800-40 provides guidance on security patch installation.</p>	(b)(7)(E)	

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SI-3	Malicious Code Protection [Virus Protection]	Verify that the information system implements malicious code protection that includes a capability for automatic updates.	<p>The organization employs virus protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.</p> <p>The organization uses the virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) transported:</p> <p>(i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks), or other common means</p> <p>(ii) by exploiting information system vulnerabilities</p> <p>The organization updates virus protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.</p> <p>Consideration is given to using virus protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).</p>	(b)(7)(E)	
SI-4	Intrusion Detection Tools and Techniques	Verify that the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	Intrusion detection and information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, virus protection software, log monitoring software, network forensic analysis tools).		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SI-5	Security Alerts and Advisories (b)(7)(E)	Verify that the organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.	The organization documents the types of actions to be taken in response to security alerts/advisories.	(b)(7)(E)	
SI-6	Security Functionality Verification	Verify that the information system verifies the correct operation of security functions upon system startup and restart, upon command by user with appropriate privilege, periodically, etc., and either notifies system administrator, shuts the system down, restarts the system, etc., when anomalies are discovered.	Determine if the system verifies the correct operation of security functions upon system startup and restart, and/or upon command by users with appropriate privileges. Determine if the system notifies the system administrator, shuts the system down, or restarts the system when anomalies are discovered. Examine policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the verification of security functions within the information system is performed correctly. Verify that failed security test results are provided to the appropriate organizational personnel.		
SI-7	Software and Information Integrity	Verify that the information system detects and protects against unauthorized changes to software and information.	The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SI-8	SPAM AND SPYWARE PROTECTION (b)(7)(E)	Verify that the information system implements spam and spyware protection.	<p>The organization employs spam and spyware protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.</p> <p>The organization uses the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks), or other common means.</p> <p>Consideration is given to using spam and spyware protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).</p>	(b)(7)(E)	
SI-9	INFO INPUT RESTRICTIONS (b)(7)(E)	Verify that the organization restricts the information input to the information system to authorized personnel only.	Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.		
SI-10	INFO INPUT ACCURACY, COMPLETENESS, AND VALIDITY [Reconciliations]	Verify that the information system checks information inputs for accuracy, completeness, and validity.	<p>Checks for accuracy, completeness, and validity of information should be accomplished as close to the point of origin as possible.</p> <p>Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
			Inputs passed to interpreters should be prescreened to ensure the content is not unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, and validity of information inputs should be guided by organizational policy and operational requirements.	(b)(7)(E)	
SI-11	ERROR HANDLING (b)(7)(E)	Verify that the information system identifies and handles error conditions in an expeditious manner.	The structure and content of error messages should be carefully considered by the organization. User error messages generated by the information system should provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages should be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions should be guided by organizational policy and operational requirements.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SI-12	INFORMATION OUTPUT HANDLING AND RETENTION	Verify that the organization handles and retains output from the information system in accordance with organizational policy and operational requirements.	<p>Determine if the organization retains output from the information system in accordance with organizational policy and procedures.</p> <p>Determine if specific parties are assigned responsibility and specific actions are defined to ensure that information output handling and retention are correctly implemented within the information system.</p> <p>Determine: (i) if information output handling and retention are consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during information output handling and retention are being documented and the resulting information used to actively improve the information output handling and retention policy, procedures and processes on a continuous basis.</p>	(b)(7)(E)	
MP-1	Media Protection Policy and Procedures (b)(7)(E)	<p>Verify that the organization develops, disseminates, and periodically reviews/updates:</p> <p>(i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance</p> <p>(ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls</p>	<p>The media protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization.</p> <p>Media protection procedures can be developed for the security program in general, and for a particular information system, when required.</p> <p>NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>		
MP-2	Media Access	Verify that the organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.			

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
MP-3	Media Labeling	<p>Verify that the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information.</p> <p>The organization exempts specific types of media or hardware components from labeling so long as they remain within a secure environment.</p>	<p>The organization marks human-readable output appropriately in accordance with applicable policies and procedures.</p> <p>At a minimum, the organization affixes printed output that is not otherwise appropriately marked, with cover sheets and labels digital media with the distribution limitations, handling caveats, and applicable security markings, if any, of the information.</p>	(b)(7)(E)	
MP-4	Media Storage	<p>Verify that the organization physically controls and securely stores information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.</p>	<p>The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.</p> <p>The organization protects unmarked media at the highest FIPS 199 security category for the information system until the media are reviewed and appropriately labeled.</p>		
MP-5	Media Transport	<p>Verify that the organization controls information system media (paper and electronic) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.</p>			
MP-6	Media Sanitization	<p>Verify that the organization sanitizes information system digital media using approved equipment, techniques, and procedures.</p> <p>The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.</p>	<p>Sanitization is the process used to remove information from digital media such that information recovery is not possible. Sanitization includes removing all labels, markings, and activity logs.</p> <p>Sanitization techniques, including degaussing and overwriting memory locations, ensure that organizational information is not disclosed to unauthorized individuals when such media is reused or disposed. Refer to NIST Special Publication 800-36.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
MP-7	Media Destruction and Disposal	Verify that the organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media.	<p>The organization:</p> <p>(i) sanitizes information system hardware and machine-readable media using approved methods before being released for reuse outside of the organization</p> <p>(ii) destroys the hardware/media</p> <p>Media destruction and disposal should be accomplished in an environmentally approved manner.</p> <p>The National Security Agency provides media destruction guidance at http://www.nsa.gov/ia/government/mdg.cfm.</p> <p>The organization destroys information storage media when no longer needed in accordance with organization-approved methods and organizational policy and procedures.</p> <p>The organization tracks, documents, and verifies media destruction and disposal actions.</p> <p>The organization physically destroys nonmagnetic (optical) media (e.g., compact disks, digital video disks) in a safe and effective manner.</p> <p>NIST Special Publication 800-36 provides guidance on appropriate sanitization equipment, techniques and procedures.</p>	(b)(7)(E)	

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
IR-1	Incident Response Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls	The incident response policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-12 provides guidance on security policies and procedures.	(b)(7)(E)	
IR-2	Incident Response Training (b)(7)(E)	Verify that the organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually.			
IR-3	Incident Response Testing (b)(7)(E)	Verify that the organization tests the incident response capability for the information system at least annually using [organization-defined tests and exercises] to determine the incident response effectiveness and documents the results.			
IR-4	Incident Handling (b)(7)(E)	Verify that the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
IR-5	Incident Monitoring (b)(7)(E)	Verify that the organization tracks and documents information system security incidents on an ongoing basis.		(b)(7)(E)	
IR-6	Incident Reporting	Verify that the organization promptly reports incident information to appropriate authorities.	The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.		
IR-7	Incident Response Assistance (b)(7)(E)	Verify that the organization provides an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.	Possible implementations of incident support resources in an organization include a help desk or an assistance group and access to forensics services, when required.		
AT-1	Security Awareness and Training Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	The security awareness and training policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AT-2	Security Awareness	Verify that the organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter.	<p>The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access.</p> <p>The organization's security awareness program is consistent with the requirements contained in 5 C.F.R. Part 930.301 and with the guidance in NIST Special Publication 800-50.</p>	(b)(7)(E)	
AT-3	Security Training	Verify that the organization: <ol style="list-style-type: none">1. Identifies personnel with significant information system security roles and responsibilities2. Documents those roles and responsibilities3. Provides appropriate information system security training before authorizing access to the system and regularly thereafter.	<p>The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access.</p> <p>In addition, the organization ensures system managers, system administrators, and other personnel having access to system-level software have adequate technical training to perform their assigned duties.</p> <p>The organization's security training program is consistent with the requirements contained in 5 C.F.R. Part 930.301 and with the guidance in NIST Special Publication 800-50.</p>		
AT-4	Security Training Records	Verify that the organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.			

SEC CONFIDENTIAL



A.3 Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The results of ECS's evaluation of EFOIA's technical controls are shown in the last two columns of this control table. These results indicate whether the control was met or not (Yes/No/Partial) and why (Auditor's Comments).

Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
IA-1	Identification and Authentication Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls	The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73 and 800-76 (ii) other applicable federal laws, directives, policies, regulations, standards, and guidance The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.	(b)(7)(E)	

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
IA-2	User Identification and Authentication [Passwords and Tokens]	Verify that the information system uniquely identifies and authenticates users (or processes acting on behalf of users).	<p>Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.</p> <p>FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors.</p> <p>NIST Special Publication 800-63 provides guidance on remote electronic authentication. For other than remote situations, when users identify and authenticate to information systems within a specified security perimeter which is considered to offer sufficient protection, NIST Special Publication 800-63 guidance should be applied as follows:</p> <p>(i) for low-impact information systems, tokens that meet Level 1, 2, 3, or 4 requirements are acceptable</p> <p>(ii) for moderate-impact information systems, tokens that meet Level 2, 3, or 4 requirements are acceptable</p> <p>(iii) for high-impact information systems, tokens that meet Level 3 or 4 requirements are acceptable.</p> <p>In addition to identifying and authenticating users at the information system level, identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.</p>	(b)(7)(E)	
IA-3	Device Identification and Authentication (b)(7)(E)	Verify that the information system identifies and authenticates specific devices before establishing a connection.	The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
IA-4	Identifier Management [User Acct Mgmt]	Verify that the organization manages user identifiers by: (i) uniquely identifying each user (ii) verifying the identity of each user (iii) receiving authorization to issue a user identifier from an appropriate organization official (iv) ensuring that the user identifier is issued to the intended party (v) disabling user identifier after a certain period of inactivity (vi) archiving user identifiers	Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors.	(b)(7)(E)	

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
IA-5	Authenticator Management	<p>Verify that the organization manages information system authenticators (e.g., tokens, P K I certificates, biometrics, passwords, key cards) by:</p> <p>(i) defining initial authenticator content</p> <p>(ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators</p> <p>(iii) changing default authenticators upon information system installation</p>	<p>Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.</p> <p>For password-based authentication, the information system:</p> <p>(i) protects passwords from unauthorized disclosure and modification when stored and transmitted</p> <p>(ii) prohibits passwords from being displayed when entered</p> <p>(iii) enforces password minimum and maximum lifetime restrictions</p> <p>(iv) prohibits password reuse for a specified number of generations</p> <p>For P K I-based authentication, the information system:</p> <p>(i) validates certificates by constructing a certification path to an accepted trust anchor</p> <p>(ii) establishes user control of the corresponding private key</p> <p>(iii) maps the authenticated identity to the user account.</p> <p>FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication.</p>	(b)(7)(E)	

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
IA-6	Authenticator Feedback	Verify that the information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.	The information system may obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).	(b)(7)(E)	
IA-7	Cryptographic Module Authentication	Verify that for authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.			
AC-1	Access Control Policy and Procedures (b)(7)(E)	<p>Verify that the organization develops, disseminates, and periodically reviews/updates:</p> <p>(i) A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance</p> <p>(ii) Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls</p>	<p>Verify that the access control policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.</p> <p>The access control policy can be included as part of the general information security policy for the organization.</p> <p>Access control procedures can be developed for the security program in general, and for a particular information system, when required.</p> <p>NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AC-2	Account Management	<p>Verify that the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.</p> <p>Verify that the organization reviews information system accounts regularly.</p>	<p>Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations.</p> <ol style="list-style-type: none">1. Verify that the organization identifies authorized users of the information system and specifies access rights/privileges.2. Verify that the organization grants access to the information system based on:<ol style="list-style-type: none">(i) A valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria(ii) Intended system usage <p>The organization requires proper identification for requests to establish information system accounts and approves all such requests.</p> <ol style="list-style-type: none">1. Verify that the organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts.2. Verify that the organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured.3. Verify that account managers are also notified when users' information system usage or need-to-know changes.	(b)(7)(E)	

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AC-3	ACCESS ENFORCEMENT	Verify that the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	<p>Access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.</p> <p>In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.</p> <p>If encryption of stored information is employed as an access enforcement mechanism, verify that the cryptography used is FIPS 140-2 compliant.</p>	(b)(7)(E)	
AC-4	INFORMATION FLOW ENFORCEMENT	Verify that the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	<p>Information flow control policies and enforcement mechanisms are employed by organizations to control the flow of information between designated sources and destinations (e.g., individuals, devices) within information systems and between interconnected systems based on the characteristics of the information.</p> <p>Simple examples of flow control enforcement can be found in firewall and router devices that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.</p> <p>Flow control enforcement can also be found in information systems that use explicit labels on information, source, and destination objects as the basis for flow control decisions (e.g., to control the release of certain types of information).</p>		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AC-5	SEPARATION OF DUTIES	Verify that the information system enforces separation of duties through assigned access authorizations.	<p>Verify that the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.</p> <p>There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion.</p> <p>Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.</p>	(b)(7)(E)	
AC-6	LEAST PRIVILEGE	Verify that the information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	Verify that the organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.		
AC-7	UNSUCCESSFUL LOGIN ATTEMPTS	<p>Verify that the information system enforces a limit of the number consecutive invalid access attempts by a user during a specific time period.</p> <p>The information system either automatically locks the account/node for a certain time period or delays next login prompt according to a delay algorithm when the maximum number of unsuccessful attempts is exceeded.</p>	Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AC-8	SYSTEM USE NOTIFICATION	<p>Verify that the information system displays an approved, system use notification message before granting system access informing potential users:</p> <p>(i) that the user is accessing a U.S. Govt information system</p> <p>(ii) that system usage may be monitored, recorded, and subject to audit</p> <p>(iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties</p> <p>(iv) that use of the system indicates consent to monitoring and recording.</p> <p>The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.</p>	<p>Verify that privacy and security policies are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.</p> <p>For publicly accessible systems:</p> <p>(i) the system use information is available as opposed to displaying the information before granting access</p> <p>(ii) there are no references to monitoring, recording, or auditing since privacy accommodations for such systems generally prohibit those activities</p> <p>(iii) the notice given to public users of the information system includes a description of the authorized uses of the system.</p>	(b)(7)(E)	
AC-9	Previous Logon Notification	Verify that the information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.	NOT SELECTED FOR BASELINE		
AC-10	Concurrent Session Control	Verify that the information system limits the number of concurrent sessions for any user to a certain number of sessions.	Verify that the information system limits the number of concurrent sessions for any user. Attempt to have more than one active session with a set of credentials, or review authentication server configuration.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AC-11	Session Lock	Verify that the information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	Users can directly initiate session lock mechanisms. The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. A session lock is not a substitute for logging out of the information system.	(b)(7)(E)	
AC-12	Session Termination	Verify that the information system automatically terminates a session after a period of inactivity.			
AC-13	Supervision and Review—Access Control	Verify that the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.	The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently, the activities of users with significant information system roles and responsibilities.		
AC-14	Permitted Actions w/o Identification or Authentication	Verify that the organization identifies specific user actions that can be performed on the information system without identification or authentication.	The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems.		
AC-15	Automated Marking	Verify that the information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.	NOT SELECTED FOR BASELINE		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AC-15	Automated Labeling (b)(7)(E)	Verify that the information system appropriately labels information in use, in storage, and in transmission.	NOT SELECTED FOR BASELINE	(b)(7)(E)	
AC-17	Remote Access (b)(7)(E)	<p>Verify that the organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions.</p> <p>Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.</p>	<p>Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access.</p> <p>The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology).</p> <p>The organization permits remote access for privileged functions only for compelling operational needs. NIST Special Publication 800-63 provides guidance on remote electronic authentication.</p>		
AC-18	Wireless Access Restrictions (b)(7)(E)	<p>Verify that the organization:</p> <p>(i) establishes usage restrictions and implementation guidance for wireless technologies</p> <p>(ii) documents, monitors, and controls wireless access to the information system.</p> <p>Appropriate organizational officials authorize the use of wireless technologies.</p>	NIST Special Publication 800-48 provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AC-19	ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES (b)(7)(E)	Verify that the organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.	Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants) are not allowed access to organizational networks without first meeting organizational security policies and procedures. Security policies and procedures might include such activities as scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).	(b)(7)(E)	
AC-20	PERSONALLY OWNED INFORMATION SYSTEMS (b)(7)(E)	Verify that the organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.	The organization establishes strict terms and conditions for the use of personally owned information systems. The terms and conditions should address, at a minimum: (i) the types of applications that can be accessed from personally owned information systems (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted (iii) how other users of the personally owned information system will be prevented from accessing federal information (iv) the use of virtual private networking (VPN) and firewall technologies (v) the use of and protection against the vulnerabilities of wireless technologies (vi) the maintenance of adequate physical security controls (vii) the use of virus and spyware protection software (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, spyware definitions)		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AU-1	Audit and Accountability Policy and Procedures (b)(7)(E)	Verify that the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls	The audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	(b)(7)(E)	
AU-2	Auditable Events	Verify that the information system generates audit records for certain events.	The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AU-3	Content of Audit Records	Verify that the information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.	Audit record content includes, for most audit records: (i) date and time of the event (ii) the component of the information system (e.g., software component, hardware component) where the event occurred (iii) type of event (iv) subject identity (v) the outcome (success or failure) of the event	(b)(7)(E)	
AU-4	Audit Storage Capacity	Verify that the organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.			
AU-5	Audit Processing	Verify that in the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes certain additional actions (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records).			

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AU-6	Audit Monitoring, Analysis, and Reporting	Verify that the organization regularly: 1. Reviews/analyzes audit records for indications of inappropriate or unusual activity 2. Investigates suspicious activity or suspected violations 3. Reports findings to appropriate officials 4. Takes necessary actions		(b)(7)(E)	
AU-7	Audit Reduction and Report Generation	Verify that the information system provides an audit reduction and report generation capability.			
AU-8	Time Stamps	Verify that the information system provides time stamps for use in audit record generation.	Time stamps of audit records are generated using internal system clocks that are synchronized system wide.		
AU-9	Protection of Audit Information	Verify that the information system protects audit information and audit tools from unauthorized access, modification, and deletion.			
AU-10	Non-repudiation	Verify that the information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).	NOT SELECTED FOR BASELINE		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
AU-11	AUDIT RETENTION	Verify that the organization retains audit logs for a certain period of time to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	NIST Special Publication 800-61 provides guidance on computer security incident handling and audit log retention.	(b)(7)(E)	
SC-1	System and Communications Policy and Procedures (b)(7)(E)	<p>Verify that the organization develops, disseminates, and periodically reviews/updates:</p> <p>(i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance</p> <p>(ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls</p>	<p>The system and communications protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.</p> <p>The system and communications protection policy can be included as part of the general information security policy for the organization.</p> <p>System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required.</p> <p>NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>		
SC-2	Application Partitioning	Verify that the information system separates user functionality (including user interface services) from information system management functionality.	The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SC-3	Security Function Isolation	Verify that the information system isolates security functions from nonsecurity functions.	<p>The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions.</p> <p>The information system maintains a separate execution domain (e.g., address space) for each executing process.</p>	(b)(7)(E)	
SC-4	Information Remnants	Verify that the information system prevents unauthorized and unintended information transfer via shared system resources.	Control of information system remnants, sometimes referred to as object reuse, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.		
SC-5	Denial of Service Protection (b)(7)(E)	Verify that the information system protects against or limits the effects of certain types of denial of service attacks.	<p>A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks.</p> <p>For example, network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks.</p> <p>Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.</p>		
SC-6	Resource Priority	Verify that the information system limits the use of resources by priority.	Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.		

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SC-7	Boundary Protection (b)(7)(E)	Verify that the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	<p>Any connections to the Internet, or other external networks or information systems, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels).</p> <p>The operational failure of the boundary protection mechanisms does not result in any unauthorized release of information outside of the information system boundary.</p> <p>Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.</p>	(b)(7)(E)	
SC-8	Transmission Integrity	Verify that the information system protects the integrity of transmitted information.	The FIPS 199 security category (for integrity) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.		
SC-9	Transmission Confidentiality	Verify that the information system protects the confidentiality of transmitted information.	The FIPS 199 security category (for confidentiality) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.		
SC-10	Network Disconnect	Verify that the information system terminates a network connection at the end of a session or after a period of inactivity.			

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SC-11	Trusted Path	Verify that the information system establishes a trusted communications path between the user and the security functionality of the system.	NOT SELECTED FOR BASELINE	(b)(7)(E)	
SC-12	Cryptographic Key Establishment and Management	Verify that the information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.	NIST SP 800-56 provides guidance on cryptographic key establishment. NIST SP 800-57 provides guidance on cryptographic key management.		
SC-13	USE OF VALIDATED CRYPTOGRAPHY	Verify that when cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.	NIST SP 800-56 provides guidance on cryptographic key establishment. NIST SP 800-57 provides guidance on cryptographic key management.		
SC-14	Public Access Protections (b)(7)(E)	Verify that for publicly available systems, the information system protects the integrity of the information and applications.			
SC-15	Collaborative Computing (b)(7)(E)	Verify that the information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).			

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SC-16	Transmission of Security Parameters	Verify that the information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.	NOT SELECTED FOR BASELINE	(b)(7)(E)	
SC-17	Public Key Infrastructure Certificates	Verify that the organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.	Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. NIST Special Publication 800-63 provides guidance on remote electronic authentication.	(b)(7)(E)	
SC-18	Mobile Code	Verify that the organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.	Mobile code (active content) technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code. Additional information on risk-based approaches for the implementation of mobile code technologies can be found at: http://iase.disa.mil/mcp/index.html .	(b)(7)(E)	

SEC CONFIDENTIAL



Ctrl No.	Control Name	Control Description	Additional Guidance	Yes / No / Partial	Auditor's Comments
SC-19	VOICE OVER INTERNET PROTOCOL (b)(7)(E)	Verify that the organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet P rotocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously (ii) documents, monitors, and controls the use of VoIP within the information system. Appropriate organizational officials authorize the use of VoIP.	NIST Special Publication 800-58 provides guidance on security considerations for VOIP technologies employed in information systems.	(b)(7)(E)	

SEC CONFIDENTIAL