Description of document:	Department of the Treasury Security Manual, TD P 15-71, 2011-2014
Requested date:	12-November-2016
Release date:	16-May-2018
Posted date:	04-March-2019
Source of document:	FOIA Request Department of the Treasury Washington, D.C. 20220 Fax: (202) 622-3895 Treasury Department online request portal: https://www.treasury.gov/foia/pages/gofoia.aspx

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

May 16, 2018

RE: 2016-06-021

VIA ELECTRONIC MAIL

This is the final response to your Freedom of Information Act (FOIA) request dated November 12, 2016, filed with the U.S. Department of the Treasury. You seek a copy of Treasury's Security Manual.

Your request has been processed under the provisions of the FOIA 5 U.S.C. § 552. Treasury's Departmental Offices conducted a reasonable search for responsive records and located 474 pages. After carefully reviewing the materials, I am releasing all 474 pages in full. Copies of the releasable pages are enclosed. There are no fees assessed at this time since allowable charges fell below $25.

If any questions arise concerning this action, please contact Karen Edwards at (202) 927-8989, or email at karen.edwards@treasury.gov. Please reference FOIA Request 2016-06-021 when inquiring.

Sincerely,

Paul Levitan

Digitally signed by Paul Levitan
Date: 2018.05.16 19:41:51 -04'00'

Paul Levitan
Director, FOIA and Transparency

Enclosure
Document set (474 pages)
Original FOIA request

General Information Updated
Treasury-wide Security Programs 6/17/11

1. Introduction

Treasury security programs consist of the following security functions including operational support for the Departmental Offices personnel security, industrial security, physical security and security education/training programs.

2. Treasury-wide Security Programs

a. *Personnel Security (Policy).* Establishes Treasury-wide minimum standards for background investigations and uniformed guidelines for adjudication of those investigations; interprets and assists bureaus in implementing governmental and departmental policy; and evaluating the effectiveness of bureau implementation.

b. *Information Security.* Establishes Treasury-wide minimum standards for safeguarding classified information and support for sensitive information. This includes protective requirements for:

- Identifying.
- Marking (including downgrading/ declassification and decontrolling).
- Handling.
- Processing.
- Storing.
- Transmitting.
- Accounting for/tracking.
- Destruction.

c. *Physical Security.* Establishes Treasury-wide minimum standards to ensure protection of Departmental personnel, facilities, and assets; and assisting and evaluating the effectiveness of bureau implementation.

d. *Industrial Security.* Establishes Treasury-wide minimum standards to protect the Department's classified and sensitive information assets, and facilities accessed by contractors throughout all stages of the acquisition process.

e. *Security Education/Training.* Establishing Treasury-wide training for persons authorized access to classified information (including annually for Original Classification Authorities identified in Treasury Order 105-19) and support for sensitive information.

f. *Counterintelligence (CI).* Establishes Treasury-wide policies to identify and deter intelligence collection activities conducted against the Department's personnel, information and programs. Also develops CI awareness training programs and coordinates CI investigations and activities with the law enforcement and intelligence communities.

General Information
Departmental Offices

Updated
6/17/11

1. Introduction

The Treasury Security Manual serves as the Departmental Offices (DO) regulations with respect to security programs administered by the Director, Office of Security Programs (OSP).

2. Departmental Offices - Operations

a. *DO Personnel Security (Operations).* Ensures the integrity and trustworthiness of the DO, Office of Inspector General (OIG), Special Inspector General for the Troubled Asset Recovery Program (TARP), TARP employees, the Office of Technical Assistance, HR Connect, and Community Development Financial Institutions workforce by:

- Initiating and adjudicating required background investigations (BI).
- Granting security clearances for access to classified information.
- Maintaining corresponding security files and electronic database records.
- Providing verification of security clearances for clients and customers.
- Adjudicating sensitive compartmented information (SCI) requests for the entire Department.

b. *DO Physical Security (Operations).* Implements Treasury and national policies for protection of DO personnel, property, and information within the Treasury Complex (Main Treasury and Annex Buildings) and DO satellite office locations. This includes:

- Access controls, badges, keys, key-cards, etc., for DO-occupied space.
- Repair/maintenance of security equipment protecting classified and sensitive information.
- Reporting/resolving security incidents, infractions and violations.
- Liaison with the United States Secret Service (USSS), Federal Protective Service (FPS), General Services Administration (GSA), et al.
- Collection/destruction of paper classified/sensitive waste.

c. *DO Information Security (Operations).* Provides required initial, annual refresher training and specialized training for employees authorized access to classified and sensitive information.

General Information
Treasury and Bureau Responsibilities

Updated 6/17/11

1. Introduction

The provisions of the Treasury Security Manual apply to the Departmental Offices (DO), all Treasury bureaus, the Office of Inspector General (OIG), the Treasury Inspector General for Tax Administration (TIGTA), the Special Inspector General for the Troubled Asset Recovery Program, the TARP, the Office of Technical Assistance, HR Connect, and Community Development Financial Institutions.

In addition to the authority defined in applicable Treasury Directives, the Director, Office of Security Programs (OSP) is responsible for the Treasury security programs described herein.

2. Personnel Security (Policy) Program Responsibilities

a. Establishing Departmental and Treasury-wide minimum standards:

(1) For background investigations.
(2) For uniform guidelines for adjudication.
(3) In determining suitability for employment.
(4) For access to classified information and in support of access to sensitive information.
(5) To maintain a central index of Department-granted security clearances.

b. Interpreting and assisting bureaus in implementing national and Treasury personnel security policies. This entails providing supplemental program advice and policy guidance through instructional memoranda addressing specific problems or topics when significant suitability or security information is developed.

c. Providing verification of security clearance and investigation information for personnel security representatives requiring Departmental accreditation to perform on-site personnel security file reviews at other Federal agencies/departments.

d. Evaluating implementation and effectiveness of Treasury and bureau-wide personnel security practices and procedures.

e. Recommending program enhancements through periodic bureau evaluations and staff visits to ensure compliance with minimum Federal personnel security program standards.

f. Developing policies to control granting security clearances for access to information or material designated "Restricted Data" and "Formerly Restricted Data" consistent with requirements of the Energy Department.

g. Representing Treasury/bureau interests on interagency forums and meetings with personnel security concerns, to share best practices, and actively promote personnel security programs within the Federal government. This includes serving as the principal contact with the Office of Personnel Management (OPM) for Treasury and with other Federal agencies and entities on personnel security matters.

h. Serving as the determination authority for eligibility for access to sensitive compartmented information (SCI) pursuant to a delegation from Treasury's Senior Official of the Intelligence Community (SOIC).

3. Information Security Program Responsibilities

a. Establishing Departmental standards to protect classified information based on Executive Order (EO) 13526, *Classified National Security Information* and Information Security Oversight Office (ISOO) directives.

b. Setting policy for protection of classified information and providing support for sensitive information.

c. Developing security training programs to promote awareness and understanding of requirements for safeguarding classified and in support of access to sensitive information by Treasury/bureau employees and those contractors and consultants providing services and/or deliverables to the Department or bureaus based on the need for access to such information. This includes providing:

(1) Security orientation for new hires.
(2) Initial security training in conjunction with authorized access to classified information.
(3) Annual refresher training.
(4) Derivative classification training.
(5) Original classification authority training.

d. Monitoring Treasury/bureau compliance with national and Treasury mandates for classified information as well as Treasury support for sensitive information. Providing classification management oversight, guidance and assistance to ensure viability of Treasury activities to safeguard classified and supporting protection of sensitive information.

e. Annually reporting on the status of Treasury's information security program and security-related costs (for classified information) to the ISOO.

f. Representing Treasury/bureau interests on interagency forums with like security concerns, to share best practices, and actively promote security programs within the Federal government.

4. Physical Security Program Responsibilities

a. Establishing Departmental standards for the physical protection of Treasury personnel, assets, operations, infrastructure, and facilities in order to ensure continued operation and fulfillment of Treasury essential functions and services.

b. Establishing Departmental standards for identifying and protecting Treasury critical infrastructure and key resources.

c. Reporting and liaising with the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and the Interagency Security Committee (ISC) on critical infrastructure physical security program issues, including reporting annual *Plan-of-Action and Milestones* and overall program status.

d. Developing Departmental standards, guidelines and training on vulnerability assessment and analysis. Advising and assisting in the analysis and selection of countermeasures, acting as liaison with external Federal and local law enforcement, and developing emergency operations.

e. Developing and administering the Treasury Security and Threat Advisory System (STAS) for the timely sharing of information concerning threats, security incidents and security guidance.

f. Providing guidance to Treasury/bureau officials and overseeing program compliance.

5. Industrial Security Program Responsibilities

a. Establishing Departmental standards and requirements for the protection of classified and sensitive information, information systems, assets, infrastructure, and facilities accessed by contractors throughout all stages of the acquisition process.

b. Establishing policies on acquisition security planning, contract administration, and security guidance to contractors. This includes guidance with respect to requirements for access to SCI by contractors.

c. Developing and issuing Departmental standards and requirements implementing the National Industrial Security Program (NISP) under EO 12829 and its implementing directives.

d. Reviewing completed Defense Department (DD) Forms 254, Contract Security Classification Specification, by all Treasury and bureau components.

e. Providing technical advice, guidance and assistance to project/contracting officers and designated security officials regarding authorization (and termination thereof) to release classified information to contractors, subcontractors, vendors, or suppliers.

f. Maintaining records on eligibility of U.S. industrial facilities and educational institutions for access to classified information.

g. Liaising with the Department of Defense (DoD), Defense Security Service (DSS) for all matters concerning Treasury/bureau contractor access to classified information and contractor security programs. This includes maintaining contact with the DSS central verification activity to obtain facility security clearance information.

h. Issuing security procedures whereby Treasury personnel security staffs might obtain personnel security clearance information from the Defense Industrial Security Clearance Office (DISCO).

i. Coordinating acquisition security policies with Treasury's Office of Procurement Executive.

j. Providing guidance and assistance to bureau security officers, their security staff, and Treasury/bureau contracting officials in interpreting and implementing acquisition security policies.

6. DO Personnel Security (Operations) Program Responsibilities

a. Ensuring integrity and trustworthiness of the DO workforce, contractors, consultants and special-hire appointees.

b. Processing and reviewing security forms for background investigations (BIs) and other required investigations.

c. Scheduling BIs to investigate service providers and monitoring progress.

d. Adjudicating results of investigations and taking appropriate follow-on actions.

e. Granting security clearances for access to classified information and maintaining security files on individual employees, contractors, and consultants.

f. Providing orientation to new hires on the clearance process and instruction for newly cleared personnel on life time non-disclosure requirements as a condition

of access to classified information and maintaining a database of employee clearance/investigative information.

7. DO Physical Security (Operations) Responsibilities

a. Providing security services in the Treasury Complex (Main Treasury and Annex Buildings) and DO satellite office locations.

b. Conducting official surveys and inquiries; preparing reports of security violations and infractions, documenting findings and recommending corrective actions as warranted.

c. Implementing Treasury security policies for safeguarding classified and in support of sensitive information.

d. Maintaining records on security equipment including locations of safes/bar-lock cabinets storing classified information and combinations.

e. Monitoring current and planned security measures to maintain the integrity of the Treasury Complex and providing security liaison to Treasury elements in DO satellite locations.

f. Developing access control policies and procedures for access to the Treasury Complex.

g. Overseeing and processing requests for DO access badges to be issued to DO employees for the Treasury Complex and credentials for senior Treasury officials.

h. Approving procurement of new security equipment; security containers, office shredders, etc.

i. Overseeing on-site collection and destruction of classified/sensitive paper waste.

j. Coordinating maintenance and repairs on security equipment safeguarding classified information and installation of locking hardware on Treasury Complex space housing secure terminals for processing classified information.

k. Liaising with the United States Secret Service – Uniformed Division in the Treasury Complex and with Federal Protective Service (FPS) security and General Services Administration (GSA) leasing/contracting officials with respect to access controls in satellite office locations housing DO employees.

8. DO Information Security (Operations) Program Responsibilities

Monitoring the DO Information Security Program to ensure compliance with Executive Order 13526 including required training, oversight, and liaison with DO policy-level offices with respect to inquiries on handling, processing, storing, copying, marking, transmission, accountability, packaging and destruction through the entire life cycle of classified information and similar processes for sensitive but unclassified information.

9. Counterintelligence (CI) Program Responsibilities

a. Establishing Departmental policies to identify and deter the intelligence collection threat from foreign security services, terrorist networks, organized crime and other inimical entities against Treasury personnel, information and programs.

b. Coordinating CI investigations and activities with the law enforcement and intelligence communities, and conducting internal CI inquiries.

c. Developing CI awareness training to alert personnel of the intelligence threat posed from foreign security services, terrorist and organized crime targeting, insider information, elicitation, insider threat and collaboration, and liaison relationships.

d. Tracking personnel adherence to CI training requirements.

e. Conducting foreign travel briefings and debriefings of personnel traveling on official business to overseas destinations (based on intelligence threat priorities) and in other circumstances when warranted.

f. Monitoring foreign visitor/press access into Treasury facilities.

g. Initiating technical security countermeasures sweeps in designated workspaces.

h. Providing CI analytical support to Treasury operations.

10. Bureau Responsibilities

Bureaus are responsible for establishing effective corresponding security programs. This includes notification to the Director, OSP of their assigned personnel handling particular security programs. Such information shall be updated as changes are made in bureau personnel and include the individual's name, phone/facsimile numbers and security clearance information.

Bureaus shall assist the Director, OSP in fulfilling that official's responsibilities with respect to Department-wide security programs. This includes providing timely responses to requests for information, reports, analyses, related statistical/cost security information and sharing their expertise with other bureaus and Federal agencies/departments, as appropriate, to assist national-level security efforts.

Within the context of personnel security, bureaus shall:

- Ensure consistent, timely and equitable personnel security and suitability determinations are made in all cases.

- Refer allegations of disloyalty or subversion to the Director, OSP who will notify the appropriate senior officials and/or will refer the allegations to the Federal Bureau of Investigation (FBI) or Treasury's Office of Inspector General (OIG), the Treasury OIG for Tax Administration (TIGTA) or the Special IG for the Troubled Asset Recovery Program (SIGTARP), when appropriate

- Consult with the Director, OSP when significant suitability information is developed concerning senior officials and particularly those with specific bureau oversight responsibilities. This includes when significant adverse information is developed prior to the issuance or recertification of security clearances.

- Inform the Director, OSP within one business day when behavioral issues are reported on those bureau employees who have been granted access to classified information.

- Maintain records of personnel security clearances granted to their employees.

- Follow the personnel security and personnel security investigations requirements established within the Treasury Security Manual (TD P 15-71).

General Information
Authorities and References

Updated
6/14/13

1. Introduction

The following national policy references and authorities are the basis for established security and related programs within the Department of the Treasury.

2. Authorities

- Executive Order (E.O.) 10450, as amended, *Security Requirements for Government Employment*, dated April 27, 1953.
- E.O. 12333, *United States Intelligence Activities*, as amended, dated June 30, 2008.
- E.O. 12829, *National Industrial Security Program*, dated January 6, 1993.
- E.O. 12968, *Access to Classified Information*, dated August 2, 1995.
- E.O. 12977, *Interagency Security Committee*, dated October 19, 1995.
- E.O. 13010, *Critical Infrastructure Protection,* dated July 15, 1996.
- E.O. 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*, dated October 8, 2001.
- E.O. 13231, *Critical Infrastructure Protection in the Information Age,* dated October 16, 2001.
- E.O. 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information,* dated June 30, 2008.
- E.O. 13526, *Classified National Security Information*, dated December 29, 2009.
- E.O. 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities,* dated August 18, 2010.
- E.O. 13556, *Controlled Unclassified Information,* dated November 4, 2010.
- Presidential Decision Directive NSC-12, *Security Awareness and Reporting of Foreign Contacts,* dated August 5, 1993.

- Transmittal No. 99-01, *Whistleblower Protection Act*, dated May 5, 1999 and Whistleblower Protection Enhancement Act of 2010.
- Presidential Policy Directive 19, *Protecting Whistleblowers with Access to Classified Information,* dated October 10, 2012.
- Presidential Policy Memorandum for Executive Departments and Agencies, *Upgrading Security at Federal Facilities*, dated June 28, 1995.
- Interagency Security Committee (ISC) Security Standards for Leased Space, September 29, 2004.
- ISC Security Design Criteria for New Federal Office Buildings and Major Renovation Projects, September 29, 2004.
- General Services Administration (GSA) Facilities Standards for the Public Buildings Service (PBS-P100), March 2003.
- National Capital Planning Commission (NCPC) report, *Designing for Security in the Nation's Capital*, October 2001.
- Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated December 2003.
- Homeland Security Act of 2002, *Creation of the Department of Homeland Security.*
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection.*
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors.*
- Homeland Security Presidential Directive 20, *National Continuity Policy.*
- National Industrial Security Program Operating Manual, reissued February 28, 2006.
- 5 Code of Federal Regulations (CFR) Part 731, *Suitability,* Part 732, *National Security Positions,* and Part 736, *Personnel Investigations.*

- 10 CFR Part 73.21, *Requirements for the Protection of Safeguards Information.* (This applies to nuclear energy classified and restricted data).
- 15 CFR Part 4a, *Classification, Declassification and Public Availability of National Security Information.*
- 31 CFR Part 2, National Security Information, §2.1 *Processing of Mandatory Declassification Review Requests* and §2.2 *Access to Classified Information by Historical Researchers, former Treasury Presidential and Vice Presidential appointees, and former Presidents and Vice Presidents.*
- 32 CFR, Part 147, *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.*
- 32 CFR Parts 2001 and 2003, *Classified National Security Information* (implementing E.O. 13526), dated June 22, 2010.
- 41 CFR Part 101-20.103, *Physical Protection and Building Security.*
- 5 United States Code (U.S.C.) 552a, *Freedom of Information Act.*
- 5 U.S.C. 552a, Public Law 93-579, *Privacy Act of 1974.*
- 5 U.S.C. 7532, *Suspension and Removal.*
- 18 U.S.C. 798, *Disclosure of Classified Information.*
- 18 U.S.C. 1924, *Unauthorized Removal and Retention of Classified Documents or Material.*
- 35 U.S.C. 181-188, *Invention Secrecy Act of 1951, as amended.*
- 42 U.S.C. 2011 *et seq., Atomic Energy Act of 1954, as amended.*
- 42 U.S.C. 13041, *Requirement for Background Checks for Employees Providing Child Care Services in Federal Facilities.*
- 50 U.S.C. 435, *Procedures Governing Access to Classified Information.*
- 50 U.S.C. 783, *Offenses Concerning Communication of Classified Information by Government Officer or Employee to an Agent or Representative of a Foreign Government.*

- Intelligence Community Directive 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,* dated September 15, 2008.

- Intelligence Community Directive 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and other Controlled Access Program Information,* dated October 1, 2008.

- Intelligence Community Directive 705, *Sensitive Compartmented Information Facilities,* dated May 26, 2010.

- Director of Central Intelligence Directive 6/1, *Security Policy for Sensitive Compartmented Information and Security Policy Manual,* dated March 1, 1995 (with administrative corrections dated November 4, 2003 and amendment dated July 12, 2006.

- Director of Central Intelligence Directive 1/20, *Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information*, dated December 29, 1991.

- Department of Defense 5220.22M, *National Industrial Security Program Operating Manual (NISPOM).*

- Treasury Order 105-19, *Delegation of Original Classification Authority; Requirements for Declassification and Downgrading*, dated June 27, 2011. This item is included within the consolidated Treasury Classification Guide.

- Treasury Directive 40-01, *Responsibilities of and to the Inspector General*, dated September 21, 1992.

- Secretary of the Treasury Delegation, dated January 3, 2005, establishing the Deputy Assistant Secretary for Security as Acting Senior Agency Official when the position of Assistant Secretary (Intelligence and Analysis) is vacant or when that official is unable to perform the functions and duties of the Senior Agency Official.

3. References

- ISOO Marking Booklet for identifying required markings for classified information at http://thegreen.treas.gov/policies/Resources/ISOO%202010%20Marking%20Booklet.pdf.

- Department of the Treasury Classification Guide, dated March 3, 2012, at http://thegreen.treas.gov/policies/Resources/Treasury%20Security%20Classification%20Guide.pdf.

- Reference Guide for Classified and Sensitive Information, dated August 2004, at http://thegreen.treas.gov/policies/Resources/Classified%20Information%20User%20Reference.pdf.

- Security Responsibilities, Do's and Don'ts pamphlet, dated October 2004, at http://intranet.treas.gov/security/publications/security_dos.pdf.

- Security Vignettes, Security Training Modules, Security Briefings, "Treasury Tales" and Security Posters at http://thegreen.treas.gov/programs/Pages/training.aspx.

Table of Contents

Updated 6/14/13

General Information

Chapter I – Personnel Security

Chapter II – Personnel Security Investigations

Chapter III – Information Security

Chapter IV – Industrial Security

Chapter V – Physical Security

Chapter VI – Counterintelligence

Chapter VII – Departmental Offices Physical Security

3. Departmental Offices Security Clearance Verification
4. Procedures for Issuing Courier Cards and Credentials in the Departmental Offices
5. Check-list for Security Inspections and Surveys
6. Schedule for Main Treasury Complex Entrances

Chapter VIII

1. Glossary of Security Terms
2. Abbreviations

Chapter I **Position Sensitivity and Risk Designation** Updated
Section 1 3/28/14

1. Introduction

The purpose of this section is to provide policy for the designation of national security and public trust positions within the Department of the Treasury for national security and covered positions. It defines the procedures and responsibilities within Departmental Offices (DO)/bureaus for designating these positions and for ensuring the implementation of the Position Sensitivity/Risk Designation requirements. Proper position designation is required to support Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information" initiatives under the Joint Security and Suitability Reform.

Every position in DO/bureaus shall be designated at either of the following two levels:

- Suitability risk levels commensurate with public trust responsibilities and attributes of the position as they relate to the efficiency of the service, and as described in Title 5 Code of Federal Regulations (CFR) Part 731.

- National Security sensitivity levels commensurate with the potential adverse impact upon the National Security that the incumbent could effect, as described in 5 CFR Part 732.

2. Responsibilities

a. *Personnel Security Office.* When personnel are recruited or when new positions are created, position sensitivity/risk level designations shall be reaffirmed or determined by the responsible DO/bureau Personnel Security Office. The Personnel Security Office or other designated organization shall ensure that the position sensitivity/risk levels are documented. The appointing personnel office shall ensure that vacancy announcements reflect the appropriate sensitivity level, requisite background investigation, and clearance level, if applicable. Position sensitivity designations established at the time of the vacancy announcement may not be changed to a higher sensitivity level for a minimum of 12 months after a hiring action. Any sensitivity designation change must be supported by changes in the official duties/responsibilities of that position that are applicable to the criteria established by OPM and consistent with existing authorities and approved by the cognizant DO/bureau security office.

b. The Director, Office of Security Programs (OSP) is responsible for making all position sensitivity determinations for DO/bureau positions and retains position sensitivity designation authority for (1) all DO/bureau presidential appointees requiring confirmation by the Senate; (2) heads of bureaus and their first deputies;

and (3) DO/bureau personnel security officers and any official with delegated authority to grant security clearances.

c. *Bureau Personnel Security Office.* Bureaus have delegated authority to designate position sensitivity for their personnel/positions, except as identified in (b) above, within their organization. The Personnel Security Office shall make all final determinations of position sensitivity in accordance with applicable guidance.

d. *Supervisory Officials.* Supervisory officials with sufficient knowledge of duty assignments and changes may recommend position sensitivity designations and any changes, subject to final approval of the DO/bureau Personnel Security Office.

e. *Bureau Personnel Officers.* The personnel officials within each bureau can make the preliminary determination of position sensitivity designations, but the final determination shall be made by the bureau Personnel Security Office.

3. Scope of the Risk Designation System

a. The Risk Designation System is used to determine position designation of National Security Positions, competitive service positions, where the incumbent can be noncompetitively converted to the competitive service, and initial career appointments in the Senior Executive Service (SES). To ensure that positions are designated uniformly and consistently by Federal agencies the system provides a systematic way of obtaining uniformity in the assessment of risk and national security sensitivity and is based on a combined assessment of the following:

(1) *Determination of General Risk Criteria* for placement of agency, programs, and positions.

(2) *Application of Criteria* for each of the following:

- Suitability.
- Information Technology (IT) Systems/Automated Information. Systems.
- National Security.

(3) *Obtaining Final Position Risk Level* for each of the following:

- Public Trust Levels:
  - High Risk.
  - Moderate Risk.
  - Low Risk.

- National Security Sensitivity Levels:
  - Special-Sensitive.
  - Critical-Sensitive.
  - Non-Critical Sensitive.
  - Non-Sensitive.

b. When the position is fully or predominantly involved in national security/access to classified information, the criteria and designation procedures in 5 CFR Part 732 apply in full and may also require consideration of the criteria in 5 CFR Part 731.

4. Risk Designation System

The Risk Designation System was developed by the Office of Personnel Management (OPM) for agencies to use in determining the proper level of investigating and screening required based on an assessment of risk and national security sensitivity. The Position Designation and Automated Tool is available at the OPM website at www.opm.gov/investigations. The four-step process below will result in a final designation, which in turn, will dictate the investigative requirements for the position in question.

a. Access the Nature of the Position

1. *National Security Requirements.* When duties of the position require eligibility for access to classified information or could otherwise impact the national security, or;

2. *Suitability Requirements.* Assessment of public trust responsibilities is required for covered positions.

b. Determine the potential impact of the position on the efficiency or integrity of the service (Public Trust).

c. Use the point adjustment system for program designation and level of supervision.

d. Identify the final position designation and required investigation.

5. Public Trust Positions

a. Public trust positions are those in which the incumbent has the potential to affect the integrity, efficiency, and effectiveness of assigned U.S. Government activities. The potential for adverse affect includes their action or inaction that could diminish public confidence, whether or not actual damage occurs.

b. These positions generally include policy-making, rulemaking, major program responsibility, law enforcement, public safety and health, fiduciary responsibilities, or other duties and responsibilities demanding a significant degree of public trust. These positions usually do not directly involve national security and are not typically occupied by an incumbent that requires a national security clearance.

See Exhibit 1. Suitability Position Risk Levels, for additional information to support this process.

6. National Security Positions

National security positions are those that (1) involve activities of the U.S. Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, foreign relations, and related activities concerned with the preservation of the military and economic strength of the United States; and (2) that require regular use of, or access to, classified information.

A position within the context of national security is defined as one in which an incumbent could cause damage to the national security by virtue of the nature of the position. Positions designated "Special-Sensitive" are those with the potential to cause "inestimable damage" to the national security and the employee would have access to Sensitive Compartmented Information (SCI) or Special Access Programs (SAPS) created by a non-Treasury agency.

See Exhibit 2, National Security Risk Criteria and Levels, for additional information on how the three sensitivity levels are applied. The fourth level addresses non-sensitive positions.

7. Movement of an Individual from Public Trust to National Security Position

a. When an employee who occupies a public trust position and who previously has completed the Standard Form (SF) 85P, *Questionnaire for Public Trust Positions*, (and was investigated for that purpose) is subsequently determined to require a security clearance to perform assigned duties, the following shall be done:

(1) The individual public trust position should be re-designated to the appropriate national security sensitivity level, commensurate with the required security clearance.

(2) The employee shall execute a SF 86, *Questionnaire for National Security Positions*, and meet the necessary security clearance investigative criteria.

(3) When a position risk shifts from public trust to national security and a security clearance is required, the investigation may be upgraded, depending on the level of security clearance required, to ensure that it meets the criteria both for the national security clearance level and the public trust risk level. Conversely, if national security duties and responsibilities are no longer part of a position, the position then reverts to its public trust risk level designation.

8. IT Systems and AIS Position Risk Criteria and Levels

a. The Office of Management and Budget (OMB) Circular No. A-130, *Management of Federal Information Resources*, dated November 30, 2000, mandates the following:

(1) The Director, OPM maintains personnel security policies for Federal personnel associated with the design, programming, operation, maintenance, or use of Federal IT/AIS.

(2) DO/bureau policies and procedures for the security of Federal IT/AIS must conform to the OPM guidance.

b. The IT/AIS risk levels and criteria, shown at Exhibit 3, shall be used as an integral part of Suitability and Security Position Risk Designation Systems.

c. All contractor personnel having access to information or passwords associated with DO/bureau IT/AIS designated sensitive, including off-worksite access, shall be subject to the risk designation system that is applicable to Federal employees.

9. Relationship between Suitability Risk Levels and National Security Sensitivity Levels

With very few exceptions, National Security positions (exclusive of suitability) relate to requirements for access to classified information. Therefore, National Security position sensitivity designations shall include suitability considerations.

10. Position Sensitivity for Foreign Duty Assignments

The sensitivity of DO/bureau positions at duty stations outside the United States or its possessions shall be designated, at a minimum, Critical-Sensitive because the incumbents will require regular or frequent access to Department of State diplomatic facilities.

11. Contractors and Position Sensitivity/Risk Level Designations

The personnel security screening for contractors shall be consistent with that required for Federal employees who occupy the same positions and have the same position sensitivity designation, as stated in Executive Order 13467. The necessity for personnel security screening shall be included as a specification in all contracts.

12. Risk Designation System—Position Sensitivity

a. The position sensitivity and risk level designation of a position must be based on an overall assessment of the damage that an individual, by virtue of occupying the position, could cause to National Security or to the efficiency or integrity of DO/bureau operations, also known as "the efficiency of the service."

b. When recruitment actions are taken or when new positions are created, position sensitivity/risk level designations shall be reaffirmed or determined by the responsible DO/bureau Personnel Security Officer. The organization wherein the position lies shall record the appropriate designation in coded form (1N or 1C through 6N or 6C) in Block 12 on the Optional Form (OF) 8, *Position Description*, and on the SF 52, *Request for Personnel Action*. The appointing personnel office shall ensure the position sensitivity/risk level is recorded on the SF 50, *Notification of Personnel Action*.

c. Vacancy announcements shall note when positions require a security clearance and/or involves access to SCI or special access programs. The announcement must also specify that the individual selected for the position is required to be able to obtain AND maintain national security eligibility as a condition of employment.

d. DO/bureaus must utilize a consistent and uniform method for determining the risk level of positions within their respective organization. If a bureau develops its own system or adopts a system for designating positions, the system shall be documented and maintained, just as the OPM system is documented and maintained in procedural guidance. Use of a system other than the OPM system, requires the approval of the Director, OSP. See Exhibit 4 for information regarding the codes that shall be used in all DO/bureau offices.

13. Management Survey (For Position Risk Designation)

a. The Position Designation Record shall be completed for each DO/bureau position and maintained by that organization. The DO/bureau human resources/personnel offices will maintain a record of Public Trust suitability designations. These designations also shall be maintained by the DO/bureau Personnel Security Office.

b. The Management Survey (For position risk designation) is subject to review by the Director, OSP and by OPM during periodic audits/evaluations of DO/bureau suitability programs, or on a case-by-case basis, as required. This is to ensure that DO/bureaus are considering all the pertinent factors when designating positions relative to the efficiency of the service.

Exhibit 1. Examples of Suitability Position Risk Levels

Risk Levels	Definitions and Representative Duties/Responsibilities
High Risk (HR) **Public Trust Position**	**Positions that have the potential for *exceptionally serious impact on and/or damage to* the efficiency of the service.** The duties of the position are especially critical to the Department of the Treasury or a program mission with broad scope of policy or program authority. Positions include: • Policy-making, Government rulemaking, and program responsibility; • Higher level management duties/assignments, or major program responsibilities; • Independent spokespersons or non-management positions with authority for independent action; • Investigative, law enforcement, or any position that requires carrying of a firearm; or • Fiduciary, public contact or other duties demanding the highest degree of public trust.
Moderate Risk (MR) **Public Trust Position**	**Positions that have the potential for *moderate to serious impact on and/or damage* to the efficiency of the service.** The duties of the position are considerably important to the Department of the Treasury or a program mission with significant program responsibility, or delivery of customer services. Positions include: • Assistants to policy development and implementation; • Mid-level management assignments; • Non-managerial positions with authority for independent or semi-independent action; • Delivery of service positions that demand public confidence or trust; or • Persons who provide child care services.
Low Risk (LR)	**Positions that involve duties and responsibilities having *limited relationship* to the agency or program mission.** The duties of the position have the potential for ***limited impact* on *and/or damage to*** the efficiency of the service.

Exhibit 2. National Security Risk Criteria and Levels

Levels	National Security Risk Criteria
Special-Sensitive (SS)	Positions with the potential to cause inestimable damage to the national security, including: • Access to Sensitive Compartmented information (SCI); • Access to any other intelligence related Special Sensitive information or involvement in Top Secret Special Access Programs (SAP) • Any position that an agency head determines to be in a higher level than Critical-Sensitive because of special requirements.
Critical-Sensitive (CS)	**Positions with potential to cause exceptionally grave damage to the national security, including:** Positions that involve any of the following: • Access up to and including **TOP SECRET** or "Q" classified information; • Development or approval of war plans, or plans/particulars of future, major or special operations of war, or critical and extremely important items of war; • National Security policy-making or policy-determining positions whose duties have the potential to cause exceptional or grave damage to the national security; • Investigative duties, that have the potential to cause exceptional or grave damage to the national security; • Issuance of personnel security clearances; • Duty on security boards; and • Any other positions related to national security requiring the same degree of trust.
Non Critical-Sensitive (NCS)	**Positions with the potential to cause damage to the national security, up to and including damage at the significant or serious level, including:** • Access up to and including **SECRET** or **CONFIDENTIAL** classified information; • Duties that may directly or indirectly cause harm to the national security to a moderate degree.
Non-Sensitive	**No potential for impact on and/or damage to the National Security.** Equates to a Low Risk position designation.

Exhibit 3. IT/AIS Risk Levels and Criteria

Computer/AIS Risk Levels	Adverse Impact on Computer/AIS Security
High Risk (HR) Public Trust Position	**Potential for *exceptionally serious impact.*** Involves duties especially critical to the Treasury mission with broad scope and authority with major program responsibilities that affect a major IT/AIS system. For example, a system administrator, data base administrator or network administrator might be High Risk.
Moderate Risk (MR) Public Trust Position	**Potential for *moderate to serious impact.*** Involves duties of considerable importance to the Treasury mission with significant program responsibilities that affect large portions of an IT/AIS system. For example, a programmer, systems analyst or user of a system containing financial, proprietary or privacy act information might be Moderate Risk.
Low Risk (LR)	**Potential for impact involving duties of *limited relationship*** to the DO/bureau mission through the use of IT/AIS system. For example, an e-mail or word processing use might be Low Risk.

Exhibit 4. Codes for Risk Level and Sensitivity Level

Risk Level	Code	Sensitivity Level	Code
High Risk (Non-IT/AIS)	6N	Special-Sensitive (Non-IT/AIS)	4N
High Risk – IT/AIS	6C	Special-Sensitive – IT/AIS	4C
Moderate Risk (Non-IT/AIS)	5N	Critical-Sensitive (Non-IT/AIS)	3N
Moderate Risk – IT/AIS	5C	Critical-Sensitive – IT/AIS	3C
Low Risk (Non-IT/AIS)	1N	Noncritical-Sensitive (Non-IT/AIS)	2N
Low Risk – IT/AIS	1C	Noncritical-Sensitive – IT/AIS	2C
		Non-sensitive – IT/AIS	See Low Risk

Chapter I
Section 2

Issuing Clearances and Granting Access to Classified Information

Updated
3/28/14

1. Introduction

This chapter presents the guidelines for establishing the requirements within the Department of the Treasury for issuing clearances and granting access to classified information commensurate with Executive Order (EO) 12968, *Access to Classified Information.* Questions concerning personnel security policies should be referred to the servicing Departmental Offices (DO)/bureau personnel security office or other designated component. The Director, Office of Security Programs (OSP) shall provide the Department's interpretation of security policy, procedures and, as necessary, written guidance to DO/bureaus.

2. Policy

a. Eligibility for access to classified information, except in those exceptionally rare circumstances identified in paragraph 5, is limited to United States citizens for whom an appropriate investigation of their personal and professional history indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment; as well as freedom from conflicting allegiances and potential for coercion; and the willingness and ability to abide by regulations governing the use, handling, processing and protection of classified information.

b. A determination of eligibility for access to classified information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel security officials. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States and any doubt shall be resolved in favor of the national security. Determinations of eligibility for access to classified information are separate from suitability determinations with respect to the hiring or retention of persons for employment by DO/bureaus or any other personnel action.

c. Any employee, applicant or other individual granted access to classified information may be investigated at any time to ascertain whether he or she continues to meet the requirements for access.

d. No negative inference concerning the standards of EO 12968 may be raised solely on the basis of sexual orientation of the applicant or employee or on the basis of mental health counseling when making determinations of eligibility for access to classified information. However, mental health counseling, where relevant to the

adjudication of access to classified information, may justify further inquiry to determine if such access is clearly consistent with the national security.

3. General Guidance

a. Determining eligibility for Access to Classified Information.

(1) Eligibility determinations for access to classified information shall be based on information concerning the applicant or employee that is acquired through the investigation conducted pursuant to EO 12968, and/or that is otherwise available to security officials. The information shall be made part of the applicant's or employee's official security record. Applicants or employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access to classified information.

(2) Eligibility for access to classified information, except in those exceptionally rare circumstances identified in paragraph 5, shall be granted only to employees who are U.S. citizens for whom an appropriate investigation has been completed by an appropriate Government authority and favorably adjudicated.

(3) DO/bureau personnel who possess dual citizenship and/or who exercise any right, privilege or obligation of the foreign citizenship, i.e. voting in foreign elections or foreign property ownership, etc., after becoming a U.S. citizen may raise a security concern. Possession of a passport, identity card or other foreign identity-type document issued by a foreign government may be a disqualifying condition when considering an individual for a national security clearance.

(4) In order to mitigate the security concern, DO/bureau personnel who hold a foreign passport, identity card, or other foreign identity-type document such as a national identity card or its equivalent, may voluntarily destroy or surrender it to their personnel security officer (for storage in the individual's security file for the length of their DO/bureau employment) or otherwise invalidate the foreign issued passport. DO/bureau personnel who choose to voluntarily destroy, surrender to the personnel security officer, or otherwise invalidate the foreign issued passport or identity card, or other foreign identity-type document shall provide official proof of the invalidation and sign Attachment 1.

Surrendered foreign passports and equivalent items may be returned to those naturalized U.S. Government employees for travel purposes when their country of origin requires ingress/egress via that nation's passport when required by that nation's law. However, DO/bureau personnel shall

exit and enter the U.S. on their American passport while on engaged in official and unofficial travel. Surrendered foreign passports or equivalent identification shall be returned to the employee upon their departure from DO/bureau employment. DO/bureau personnel who are eligible for, but do not hold a foreign passport must sign the agreement shown in Attachment 2. By signing Attachment 2 they agree that they will only possess a U.S. passport. Breach of this agreement may result in the termination of that person's security clearance.

(5) Naturalized citizens may be considered for access eligibility in the same manner as native-born U.S. citizens.

(6) Non-employees generally will not be provided access to classified information.

(7) Interns whose length of service at Treasury is for less than 180 consecutive days generally will not be provided access to classified national security information.

(8) No person may have access to classified information within the Department of the Treasury until they have signed a Standard Form (SF) 312, *Classified Information Nondisclosure Agreement* and received contemporaneous training on the attendant security safeguards as required under EO 13526.

b. Authority to Grant Access to Classified Information.

(1) DO/bureaus have the authority to make determinations of eligibility for access to classified information for persons under their authority, and the consequent granting, denying, and revoking of security clearances and suspending access to classified information in conformity with the provisions of EO 12968.

(2) Bureaus may render interim eligibility determinations up to the SECRET level for applicants and employees. The Director, OSP retains the authority to render interim eligibility determinations for all TOP SECRET requests.

(3) Emergency access determinations authorized under EO 13526 remain the sole responsibility of the Director, OSP.

(4) The Director, OSP retains the authority to determine the eligibility for access to classified information, and the consequent granting, denying, and revoking of security clearances and suspending access to classified information for the following positions.

- All DO/bureau presidential appointees requiring confirmation by the Senate.
- Heads of Treasury bureaus and their first deputies.
- DO/bureau personnel security officers and any official with delegated authority to grant security clearances.

(5) Treasury is not authorized to establish its own special access programs. Access to classified information relating to a special access program shall be granted in accordance with procedures established by the head of the non-Treasury agency that created the program or, for programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs,) or intelligence sources and methods, by the Director of National Intelligence.

(6) The Director, OSP, as the official designee for the Assistant Secretary for Intelligence and Analysis, as the Head of the Intelligence Community Element for the Department of the Treasury serves as the Determination Authority for eligibility for access to Sensitive Compartmented Information (SCI) within DO/bureaus.

c. Limitations on Access Eligibility

(1) DO/bureaus shall keep the number of employees with access to classified information to the minimum necessary to perform official functions.

(2) Eligibility for access to classified information shall be limited to classification levels for which there is a need for access. No person shall be granted eligibility higher than needed to perform his or her official duties.

(3) No person shall be granted access to specific classified information unless that person has an actual need-to-know for that classified information

(4) Access to classified information will not be requested nor granted solely to permit entry or ease of movement into and within DO/bureau facilities. Specifically, access to classified information will not be granted based upon proximity and/or convenience, or a need to access non-classified information.

(5) No employee shall be deemed eligible for access to classified information merely by reason of Federal service or contracting, licensee, certificate holder or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

d. Initial Access

(1) Granting access to any classification level must be made on a need-for-access basis. Access authorization is permitted only when the official duties of a position or individual require such access. When that basis no longer exists, access must be canceled.

(2) A person may have access to specific classified information provided that all of the following are true:

The individual has appropriately completed an SF-86, Questionnaire for National Security Positions.

- A favorable determination of eligibility for access, based on the appropriate investigation by an authorized government authority and a favorable adjudication, has been made by an official personnel security officer.
- The person has received an initial security briefing for access to classified information contemporaneous with being issued a security clearance by the appropriate DO/bureau security officer.
- The person has executed a SF 312, *Classified Information Non-disclosure Agreement.*
- The person has a "need-to-know" the information.

e. Access Reinstatement

When an individual retires or is otherwise separated from the employment that resulted in the original clearance, access is terminated. If a new need for access arises, access eligibility up to the same level shall be re-approved without further investigation if the following conditions are satisfied:

(1) An investigation was completed within the prior five years and the individual received a favorable adjudication.

(2) The individual has not been separated from U.S. Government employment for more than two years.

(3) The individual certifies in writing that there has been no change in the relevant information provided by the individual for the last background investigation.

(4) There is no known information tending to indicate the individual may no longer satisfy the standards for access to classified information.

f. Reciprocal Acceptance of Access Eligibility Determinations

Unless DO or a bureau has information indicating that an applicant may not satisfy the requirements in EO 12968, it is Treasury Department policy that background investigations and eligibility determinations conducted by other U.S. Government agencies shall be mutually and reciprocally accepted.

Except where there is information indicating that an employee may not satisfy the requirements in EO 12968, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined by the Director, OSP or have an existing access eligibility re-adjudicated, so long as the employee has a need for access to the information involved.

g. Temporary or One-Time Access to Higher Levels of Classified Information

In accordance with section 2.1(b)(3) and 2.3(a), EO 12968, when an urgent operational or contractual emergency may arise for an employee or contractor to have one-time or short term access to classified information at a level higher than that for which eligible, and processing the individual to upgrade the security clearance would not be practical in a particular situation, the employee or contractor may be granted access at one security classification level above that for which eligible, subject to the following terms and conditions.

(1) One-time access may only be granted by the Director, OSP based upon sufficient justification provided by the cognizant supervisor.

(2) The individual granted one-time access must be a U.S. citizen, have a current and final DO/bureau security clearance, and have been continuously employed by the DO/bureau or a cleared DO/bureau contractor for the preceding 24-month period. One-time access is not authorized for part time or temporary employees, interns or those currently possessing an interim security clearance.

(3) Review of locally available records has been conducted and revealed no disqualifying information.

(4) Whenever possible, access will be limited to a single instance or, at most, a few rare occasions. If repeated access is required, the proper personnel security investigation must be initiated.

(5) Approval for access will automatically expire no later than 10 calendar days from the date access commenced. If the need for access is expected to continue for a period in excess of 30 days, written approval is required from the Director, OSP or appropriate bureau security officer. If the need for access is expected to extend beyond 30 days, the appropriate personnel

security investigation to support the needed security clearance should be initiated. Access will not be extended, in any case, beyond 90 days from the date access commenced, unless a supporting personnel security investigation has been requested.

(6) Access at the higher level will only be allowed under the supervision of a properly cleared DO/bureau employee. The supervisor will be responsible for recording the higher-level information actually revealed along with the dates access is afforded and will retrieve the accessed material on a daily basis and ensure its proper safeguarding.

(7) Access at the next higher level will not be authorized for Communications Security (COMSEC), Sensitive Compartmented Information (SCI), North Atlantic Treaty Organization (NATO), or another agencies Special Access Program or foreign government information.

(8) This provision will be used sparingly. Repeated use of one-time access within any three month period on behalf of the same individual is prohibited.

The Director, OSP or bureau personnel security officer, as appropriate, will maintain a record for each employee or contractor authorized one-time access. The record will include the following information:

(1) The name and social security number of the individual;

(2) The level of access authorized;

(3) Justification for the access to include an explanation of the compelling reason(s) to grant the higher-level access and, specifically, how the DO/bureau mission would be furthered;

(4) An unclassified description of the specific information to which access was afforded and the duration of the access, to include the specific dates access is afforded;

(5) A listing of the locally available records reviewed and a statement that no significant adverse information concerning the employee or contractor is known to exist; and,

(6) Identification of any pertinent security briefings/debriefings or other training given to the employee or contractor.

h. Interim Confidential or Secret Access

(1) In exceptional circumstances where official functions must be performed

prior to the completion of the final investigation interim access may be granted to an applicant or employee while the initial investigation is underway. Interim access to Confidential or Secret information may be granted under the following conditions.

- A review of the individual's current SF86 discloses no potentially disqualifying or questionable information;
- An appropriate background investigation is scheduled prior to issuance of interim Confidential or Secret access;
- A favorable National Agency Check to include a Federal Bureau of Investigation (FBI) National Criminal History Check (fingerprint check) adjudicated by appropriate approved/authorized automated procedures or trained security personnel is conducted prior to issuance of interim Confidential or Secret access; and
- Upon a written justification by the cognizant supervisor.

(2) If interim access is granted, the initial investigation must be expedited and the applicant or employee shall be notified in writing that access is expressly conditioned on the favorable completion of the investigation and a determination that the individual is eligible for access to classified information. Interim access to SCI is not authorized in any circumstance.

(3) Exceptions to paragraph 3h bullets (1) and (2) above, shall be approved in writing by the Director, OSP.

(4) Interim Top Secret. In exceptionally rare circumstances, interim eligibility to Top Secret information may be granted to an employee only when official functions must be performed prior to the completion of the final investigation and such functions require access to Top Secret information. The granting of interim access to Top Secret information is the sole responsibility of the Director, OSP and may be granted under the following conditions:

- The employee has a current and favorably adjudicated SECRET eligibility determination;
- A review of an appropriately completed and current SF-86 discloses no potentially disqualifying information;
- The appropriate background investigation has been scheduled; and
- A written justification by appropriate Assistant Secretary level or Bureau Head equivalent is provided to (and approved by) the Director, OSP.

i. Review of Access Determinations (Periodic Reinvestigations)

(1) Employees who are eligible for access to classified information shall be subject to periodic reinvestigations and may also be reinvestigated and/or re-adjudicated if there is reason to believe they may no longer meet the standards for access.

(2) Access to classified information shall be administratively terminated when an applicant or employee no longer has a need for access. Any determination made to terminate access to classified information under the authority of this paragraph shall be discretionary and final.

(3) In accordance with section 5.2(a), EO 12968, an applicant or employee may have his or her eligibility for access denied or revoked if it is determined that he or she does not meet the standards for access to classified information. (See Chapter I, Section 5, *Suspension of Access to Classified Information* for specific steps required to ensure "due process" in determining an individual's continued access).

4. Contractor Access

a. Personnel who are subject to a contract or grant or are rendering consultant services under the authority of the DO/bureaus, and who require access to classified information, shall be cleared for such access through the National Industrial Security Program (NISP). No contractor will be granted access to classified information if the contract, grant, or services to be rendered does not require access to classified information. (See Chapter II, Section 2).

b. *Personal Services* contractors (i.e., consultants or experts who contract directly with the DO/bureaus), shall be subject to the same requirements as employees for the purpose of determining position sensitivity, risk designation, and investigative requirements. They shall not be processed under the NISP.

5. Intern Access

Generally, interns will not be provided access to classified information given their limited duration at DO/bureau offices in relation to the time and resources necessary to complete an appropriate investigation, adjudication and the required individual training for access to classified information. As mentioned previously, access to classified information is discretionary and all such access must be clearly consistence with the national security interests of the United States. The Director, OSP is the approving authority for all access requests for interns. Intern access may be granted under the following conditions:

- Interns whose on-site length of service with the DO/bureau will meet or exceed a 180-day consecutive period;

- A written justification for access to classified information, including the dates of service, must be submitted by the cognizant supervisor within, but no more than 30 days prior to the intern's starting date; and

- Only Confidential or Secret access will be granted for interns.

Exceptions to this paragraph shall be approved in writing by the Director, OSP.

6. Limited Access Authorization for Immigrant Aliens and Foreign Nationals

a. Non-U.S. citizens are not eligible for a security clearance, however, access to classified information may be justified for compelling reasons in furtherance of the DO/bureau mission, including special expertise. A Limited Access Authorization (LAA) may be justified in those rare circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed and for which a cleared or clearable U.S. citizen is not available. (NOTE: LAA authorization is not a security clearance; it is a limited authorization for access to specific classified information.) When justified, a LAA may be considered under the following conditions:

- Access is limited to classified information relating to a specific project or product.

- LAAs may be granted only at the SECRET or CONFIDENTIAL level. LAAs for TOP SECRET are prohibited. Interim access is not authorized.

- The appropriate foreign disclosure authority determines that access to classified information is consistent with authority to release the information to the individual's country of origin.

- Physical custody of classified material will not be authorized.

- The LAA is not granted to an individual who will perform routine administrative or other support duties.

- The individual will not be designated as a courier or escort for classified information or material.

- The individual will not be permitted unescorted access to areas where classified information is stored or discussed. Classified information will be maintained in a location that will be under the continuous control and supervision of an appropriately cleared U.S. citizen.

- A Single-Scope Background Investigation (SSBI) is completed and covers the prior 10 years of the subject's life.

- The individual must agree to a counter-intelligence scope polygraph examination before being granted access. Failure to agree will terminate the processing of the LAA request.

b. When a LAA appears to be justified, DO/bureaus may submit a request signed by the bureau head to the Director, OSP with the following information:

- The identity of the individual for whom a LAA is requested, including: name; date and place of birth; current citizenship; social security number (if held); passport number, date of issuance, place where issued, and expiration date.

- Status as an immigrant alien or foreign national; if an immigrant alien, the date and port of entry and lawful permanent resident alien registration number (green card).

- Date and type of the most recent personnel security investigation.

- Level of access required.

- The position requiring access and the nature and identity of the specific program material (delineated as precisely as possible) for which access is requested.

- The compelling reason(s) for the request including an explanation of the special skills or special expertise the individual possesses and the rationale for not employing a cleared or clearable U.S. citizen.

- An explanation as to how the DO/bureau plans to control and limit the individual's access.

- An assessment of the risk associated with granting access to classified information.

- All security countermeasures and actions taken to mitigate the risks associated with the request.

- A statement that the candidate has agreed to undergo a counterintelligence-scope polygraph examination.

- The period of time for which access is required.

c. The Director, OSP will review the LAA request to determine if the justification provided meets the program requirements. If the justification is not adequate the LAA request will be promptly returned to the DO office or bureau. If the justification is adequate, the Director, OSP will forward the SSBI request to the appropriate investigative agency; however, the decision to authorize limited access cannot be made until favorable adjudication of the completed SSBI. The adjudication of all investigations on immigrant aliens or foreign nationals will be made by the DO OSP adjudication staff.

d. The Director, OSP will coordinate foreign disclosure decisions with the appropriate executive branch international programs offices.

e. Individuals with LAAs will be placed under the general supervision of appropriately cleared persons. Supervisors will be made fully aware of the limits to access imposed and that physical custody of classified information by the individual is not authorized. An SF 312, *Classified Information Nondisclosure Agreement* must be executed by the immigrant alien or foreign national prior to granting access to classified information.

f. Individuals who have been granted an LAA may only have access to classified information at the same or lesser level of classified information that the U.S. Government has determined may be released to the country of which the person is currently a citizen and will not be allowed to have access to any classified information other than that specifically authorized.

g. If an individual granted an LAA is transferred to another position, the LAA previously granted will be rescinded and the individual will be debriefed.

h. Periodic Re-investigation (PR) is required every five years for individuals with an LAA. Because LAA's are not authorized for more than five years, a new request for LAA must accompany a request for PR. The Director, OSP will review the justification and promptly notify the DO/bureau to either continue the LAA until favorable completion of the PR by the investigative agency or to discontinue access based on lack of justification.

i. Non-U.S. citizens are not authorized access to foreign intelligence information without approval of the originating agency, or to COMSEC keying materials, Top Secret, cryptographic, Restricted Data, or Formerly Restricted Data or another agency's Special Access Program.

6. Prohibition on Access to Classified Information for Foreign National Employees of Treasury (DO) Overseas Posts

Foreign national employees employed at Treasury/bureau overseas posts shall not be granted access to U.S. classified information.

7. Security Clearances for U.S. Executive Directors or International Financial Institutions

a. The U.S. Executive Directors and their alternates at (1) the International Bank for Reconstruction and Development (IBRD or the World Bank), (2) the Inter-American Development Bank (IADB), (3) the European Bank for Reconstruction and Development (EBRD), (4) the Asian Development Bank (ADB), (5) the International Monetary Fund (IMF), and (6) the African Development Fund (ADF) exercise their duties under the direction of the Secretary of the Treasury for any necessary access to classified information.

b. The security investigations for DO/bureau Presidential appointees that do not require Senate confirmation are initiated by Treasury's OSP. Investigations of Presidential appointees that do require Senate confirmation are initiated by the White House and conducted by the Federal Bureau of Investigation (FBI).

8. Access by Historical Researchers and Former Presidential Appointees

a. Access to classified information is limited to individuals who have a "need-to-know" the information. The requirement to limit access may only be waived in writing by the Director, OSP for persons who either are engaged in historical research, or previously have occupied policy-making positions to which they were appointed by the President.

b. Waivers may be granted only under the following conditions.

(1) When it is determined, in writing, that access is consistent with the interests of National Security.

(2) Appropriate steps are taken to protect classified information from unauthorized disclosure or compromise, and information will be protected in a manner consistent with the current requirements for safeguarding classified information.

(3) Limitations will be established to ensure that former DO/bureau Presidential appointees have access only to those classified materials that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

9. Access by Persons outside the Executive Branch

a. Classified information shall not be disseminated outside the Executive Branch

except under conditions that ensure the information will be given protections equivalent to that afforded within the Executive Branch.

b. Classified information originated by or in the custody of DO/bureaus may be made available to individuals or agencies outside the Executive Branch provided that (1) such information is necessary for performance of a function from which the U.S. Government will derive a benefit, or advantage, and (2) the release is not prohibited by the originating DO office or bureau (or foreign government in the case of Foreign Government Information).

c. Prior to the release of classified information outside the Executive Branch the following must occur:

(1) The DO/bureau shall determine the propriety of such action, in the interest of national security, and must approve the release.

(2) The Director, OSP must confirm that the recipient is eligible for access to the classified information involved and agrees to safeguard the information in accordance with the provisions of the Treasury Security Manual (TD P 15-71).

10. Reporting Significant Life Events by DO/Bureau Employees with a Security Clearance

a. Any DO/bureau employee with a security clearance (regardless of the level) shall report immediately in accordance with Standard Form 86C, Certification, (at http://thegreen.treas.gov/policies/Forms1/Electronic%20Questionnaires%20for%20Investigations%20Processing.pdf) on-line any such changes in circumstances related to Questions 1 through 29 on that form, in writing, either by email, fax, U.S Postal Service, or hand delivery, to the appropriate DO/bureau personnel security officer or other designated person. Most questions on the SF 86C are self- explainable. The following additional guidance is provided:

b. For question 9, Citizenship, DO/bureau employees shall report when assuming non-U.S. citizenship including application/receipt of a foreign passport with or without the intention to use such passport while still a Federal employee and any renunciation of U.S. citizenship.

c. For question 17, Marital Status, a DO/bureau employee who holds a TOP SECRET security clearance and who marries/cohabits (in a spouse-like relationship) during the time they ***hold such a clearance*** shall report such marriage or cohabitation to his or her appropriate personnel security officer or other designated person(s).

d. For question 21, Mental and Emotional Health, DO/bureau employees shall report

if they have consulted with a health care professional regarding an emotional or mental health condition, or were hospitalized for such a condition, or ordered by a court to undergo counseling. Counseling that is strictly for marital/family or grief unrelated to violence (by the employee), strictly related to adjustments from service in a military combat environment or strictly related to treatment as a result of a sexual assault are not required to be reported.

e. For question 22, Police Record, DO/bureau employees shall report if they have been issued a summons, citation or ticket to appear in court in a criminal proceeding against them, however, fines less than $300 for traffic offenses are not required to be reported unless the offense involves drugs or alcohol in which case further information may be required per question 23, Use of Illegal Drugs and Drug Activity.

f. For question 26, Financial Record, any DO/employee shall report declarations of bankruptcy, U.S. Government and/or court-ordered liens.

11. Administrative Actions

All DO/bureau employees and other persons who have been granted access to information, property, or other assets controlled by DO/bureaus, are subject to administrative and/or disciplinary actions for noncompliance with the provisions of the Treasury Security Manual.

12. Security Education and Supervisor/Employee Responsibilities

a. The purpose of the security education and training is to ensure that employees understand the need and procedures for protecting classified and sensitive information. The goal is to develop fundamental security habits as a natural element of each task. Adverse impact upon the national security could result from unauthorized disclosure of classified or sensitive information. Supervisor responsibilities include:

- Determining security requirements, in coordination with the Director, OSP or appropriate DO/bureau security officer for their functions and ensuring employees under their supervision understand and are well familiar with the security requirements for their particular assignments.

- Providing on-the-job security training as an essential part of security education and ensuring employees complete required training when instructed to do so.

- Continuously evaluating employees on the necessity and/or appropriateness for access to classified information or assignment to sensitive duties.

Individual responsibilities include:

- A personal, moral, and legal responsibility to protect classified and sensitive information within their knowledge, possession or control.

- Adhering to the standards of conduct required of persons holding positions of trust and avoiding personal behavior that could render them ineligible for access to classified information or assignment to sensitive duties.

- An obligation to notify their supervisor, the Director, OSP or their DO/bureau security officer, as appropriate, when they become aware of information with potential security significance regarding someone with access to classified information or assigned to sensitive duties.

- Reporting all violations of security regulations to the appropriate DO/bureau security officials.

- Comply with all security requirements set forth in the Treasury Security Manual and complete required training as instructed.

The Director, OSP and DO/bureau security officer responsibilities include:

- Instructing employees having knowledge, possession, or control of classified or sensitive information on how to determine before disseminating the information that the prospective recipient has been authorized access, needs the information to perform his or her official duties, and can properly safeguard the information.

- Advising employees of the strict prohibition against discussing classified or sensitive information over an unsecured telephone or in any other manner that may permit interception by unauthorized persons.

- Advising employees that they must report to their supervisor, the Director, OSP or DO/bureau security officer, contacts with any individual regardless of nationality, whether within or outside the scope of the individuals official activities, in which:

    - Illegal or unauthorized access is sought to classified or otherwise sensitive information;

- The employee is concerned that he or she may be the target of exploitation; or
- The employee has contact with known or suspected foreign intelligence officers from any country.

- Advising employees of the penalties for mishandling classified or sensitive information or material.

b. The following are the minimum requirements for security education:

- Indoctrination of employees upon employment by DO/bureaus in the basic principles of security.
- Contemporaneous orientation of employees when they received their security clearance to have access to classified or sensitive information at the time of assignment, regarding security requirements.
- On-the-job training in specific security requirements for the duties assigned.
- Annual refresher briefings for employees that have access to classified or sensitive information.
- Special briefings as circumstances dictate.
- Debriefing upon termination of access.

c. In accordance with EO 12968, the Director, OSP shall ensure that DO/bureaus have an effective security education and awareness program for those employees accessing classified or sensitive information.

d. DO/bureaus shall establish a method to record security education and awareness training for each individual employee as such training is completed.

13. Debriefing Program

a. Prior to an employee or other individual's departure from DO/bureaus the person will be debriefed if they: (1) held a security clearance and/or (2) had control of classified documents. The debriefing should, at a minimum, include reminders that (1) classified documents are not personal property and may not be removed from U.S. Government control, and (2) protection of classified information does not end with the person's termination of access.

DO/bureau security personnel should ensure that if an individual has signed for

documents, they are properly accounted for prior to that individual departing. Upon completion of the debriefing, DO/bureau security personnel shall request the departing individual complete the bottom portion of SF 312, *Classified Information Nondisclosure Agreement*.

b. Employees shall be debriefed in the same manner when they no longer require access to classified information.

14. Unauthorized Exposure to Classified Information

a. If an individual is inadvertently exposed to classified information, the DO/bureau security officer shall:

(1) Determine the amount of exposure to the classified information. This accounting is separate from any security inquiry into the exposure.

(2) Provide a briefing to the exposed individual regarding the requirements for protecting classified information.

(3) Provide the individual with a copy of the laws requiring him or her to protect the classified information.

(4) Have the individual sign TD F 15-05.19 *Inadvertent Disclosure Briefing and Agreement* (See Attachment 3). The completed TD F 15-05.19 shall be placed in the employee's security file.

b. If the individual declines to sign the TD F 15-05.19 the following must occur:

(1) The individual must be told that the requirement to protect the information is enforceable even without his or her signature on the form.

(2) The DO/bureau security officer shall execute a signed memo recording the fact that a briefing was given and the individual declined to sign.

15. Protecting Whistleblowers with Access to Classified Information

In accordance with Presidential Policy Directive (PDD) 19, dated October 12, 2012 employees eligible for access to classified information can effectively report waste, fraud, and abuse while protecting classified national security information free of retaliation against them for reporting such waste, fraud, and abuse. See Chapter I, Section 8.

Attachment 1

DEPARTMENT OF THE TREASURY
PASSPORT AGREEMENT BETWEEN (**NAME**) AND (TREASURY/**BUREAU**),

I, (**name**), hereby agree to adhere to the obligations contained in this Agreement if I am granted a security clearance and subsequently authorized access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order (EO) 13526, "Classified National Security Information," or under any other executive order or statute that prohibits the unauthorized disclosure of classified national security information, and unclassified information that meets the standards of classification and is in the process of a classification determination.

I understand that under EO 12968, "Access to Classified Information," eligibility for access to classified information may only be granted to those individuals who are United States citizens, and, among other qualifications whose personal and professional history affirmatively indicates loyalty to the United States. I understand and acknowledge that when an individual acts in such a way to indicate a preference for a foreign country over the United States then a concern arises as to that person's allegiance to the United States and his/her willingness to safeguard classified information. In this regard, I have been advised that conditions that raise a security concern and that may be disqualifying include the exercise of any right, privilege or obligation of foreign citizenship, including the possession and/or use of a foreign passport.

As a dual citizen of both the United States and **XXX,** I possess both a U.S. and **XXX** passport. To eliminate any appearance of foreign preference on my part I voluntarily

( ) destroyed
( ) surrendered to the personnel security officer
( ) invalidated

my passport issued by XXX. Absent consent of the Director, Office of Security Programs, Department of the Treasury, I hereby agree to use only my U.S. passport in connection with any travel (official or unofficial) while I am employed with the (U.S. Department of the Treasury or name of bureau). I understand that any breach of this Agreement may result in the termination of any security clearance I hold.

I have read this Agreement carefully and my questions, if any, have been answered. I execute this agreement voluntarily.

_____ _____
(Printed Name) (Signature and Date)

Witness_____ _____
(Printed Name) (Signature and Date)

Accepted for Treasury Department:

_____ _____
(Printed Name) (Signature and Date)

TD F 15-03.11A (8/2013)

Attachment 2

DEPARTMENT OF THE TREASURY
PASSPORT AGREEMENT BETWEEN (**NAME**) AND (TREASURY/**BUREAU**),

I, (**name**), hereby agree to adhere to the obligations contained in this Agreement if I am granted a security clearance and subsequently authorized access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order (EO) 13526, "Classified National Security Information," or under any other executive order or statute that prohibits the unauthorized disclosure of classified national security information, and unclassified information that meets the standards of classification and is in the process of a classification determination.

I understand that under EO 12968, "Access to Classified Information," eligibility for access to classified information may only be granted to those individuals who are United States citizens, and, among other qualifications whose personal and professional history affirmatively indicates loyalty to the United States. I understand and acknowledge that when an individual acts in such a way to indicate a preference for a foreign country over the United States then a concern arises as to that person's allegiance to the United States and his/her willingness to safeguard classified information. In this regard, I have been advised that conditions that raise a security concern and that may be disqualifying include the exercise of any right, privilege or obligation of foreign citizenship, including the possession and/or use of a foreign passport.

As a dual citizen of both the United States and **XXX,** I am eligible to possess both a U.S. and **XXX** passport. However, I currently only possess a U.S. passport. To eliminate any appearance of foreign preference on my part, absent consent of the Director, Office of Security Programs, Department of the Treasury, I hereby agree to continue use of only my U.S. passport in connection with any travel (official or unofficial) while I am employed with the (U.S. Department of the Treasury or name of bureau). Further, I agree that I will immediately notify the Director, Office of Security Programs of any issuance of a foreign passport in my name while I am employed by the Department of the Treasury. I understand that any breach of this Agreement may result in the termination of any security clearance I hold.

I have read this Agreement carefully and my questions, if any, have been answered. I execute this agreement voluntarily.

_____ _____
(Printed Name) (Signature and Date)

Witness_____ _____
(Printed Name) (Signature and Date)

Accepted for Treasury Department:

_____ _____
(Printed Name) (Signature and Date)

TD F 15-03.11B (8/2013)

Department of the Treasury Attachment 3

INADVERTENT DISCLOSURE BRIEFING AND AGREEMENT

Briefing for Maintaining the Security of Classified Information

1. Classified information has been either discussed with you or exposed to your view in the performance of your officially assigned duties. This disclosure on _____ was unintentional. It is therefore necessary to acquaint you with the law on this subject and for you to execute a statement binding you to secrecy in connection with any information you may have gained from this inadvertent disclosure.

2. It is impossible to overemphasize the importance of safeguarding this classified information. The time limit for safeguarding such classified information only expires upon an official U.S. Government determination that the information no longer meets the criteria for protection as national security information. Transmission or revelation of this information in any manner to an unauthorized person is prohibited by § 793 and § 794, Title 18, United States Code.

Inadvertent Disclosure Agreement

I understand that I was inadvertently exposed to classified information through no fault of my own in the performance of officially assigned duties.

I hereby affirm that I have read and understand the above instructions for maintaining the security of certain classified information. I certify that I shall never divulge to anyone else, in any manner, the classified information inadvertently exposed to me unless I have received express written permission to do so from the official custodian of the information. I understand that the transmission or revelation of this information in any manner to an unauthorized person is punishable under § 793 and § 794, Title 18, United States Code. My signature below acknowledges my understanding of the above.

_____	_____
Typed or Printed Name	Social Security Number
_____	_____
Signature	Date
_____	_____
U.S. Government Witness Signature	Date

Privacy Act Statement

The Privacy Act, 5 U.S.C. 552a, requires that Federal agencies inform individuals, at the time information is solicited from them, whether disclosure is mandatory or voluntary, by hat authority such information is solicited, and what uses will be made of the information. You are herby advised that disclosure is voluntary and the authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you more precisely, since many people appearing in the government's administrative records have the same name.

TD F 15-05.19

Chapter I
Section 3

Adjudication Guidelines

Updated
1/3/12

1. Introduction

The purpose of this section is to outline the adjudication process as found in Executive Order (EO) 12968, *Access to Classified Information*, and the Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Revised Adjudicative Guidelines), issued by the White House on December 29, 2005. This section shall be used (1) in adjudicating background investigations for all Departmental Offices (DO) /bureau applicants, employees, contractors, consultants, and other persons who require access to classified information pursuant to EO 12968, and (2) for determining eligibility for employment in a sensitive position pursuant to EO 10450, *Security Requirements for Government Employment.*

Additionally, these guidelines may be used in determining eligibility for (1) access to sensitive but unclassified information or DO/bureau information technology (IT) automated information systems (AIS),or (2) staff-like access to DO/bureau occupied facilities.

2. Adjudicative Process

The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance or assignment to sensitive duties or placement in a public trust position. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines.

The adjudicative process includes the careful weighing of a number of variables known as the "whole person concept." Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination.

a. After a thorough review, analysis, and evaluation of all available investigative information, an appropriately trained adjudicator shall determine an individual's eligibility (1) for access to classified information under EO 12968, or (2) to occupy a sensitive position pursuant to EO 10450, using the Revised Adjudication Guidelines.

b. If a security determination under EO 12968 or EO 10450 is made after a favorable initial suitability determination, the security determination shall resolve any questions of the suitability of an applicant for or an appointee to a sensitive position.

c. DO/bureaus may also determine eligibility for access to sensitive but unclassified information and/or IT/AIS using the Revised Adjudicative Guidelines.

d. A determination to grant security clearance eligibility, authorize access to classified information, or assign a person to sensitive duties or a public trust position will be based on an investigation conducted in accordance with the requirements specified in Chapter I, Section 1, of this manual.

e. Unless there is a reasonable basis for doubting a person's loyalty to the United States, decisions regarding appointment or retention in civilian employment are governed by personnel policies.

3. Contract Employees

a. In general, the responsibility for making classified access eligibility determinations for contract personnel (i.e., employees of a contractor to the agency) rests with the Defense Security Service, according to EO 12829, *National Industrial Security Program* (NISP). However, for the purpose of granting access to classified information, individuals who contract directly with DO/bureaus as consultants or experts shall not be subject to the NISP, but shall be subject to the same requirements as DO/bureau employees.

b. Determinations regarding contract personnel access to DO/bureau facilities, sensitive information, or IT/AIS, shall be made by the appropriate DO/bureau security officer, using appropriate adjudication criteria. DO/bureaus should use the Revised Adjudicative Guidelines for this purpose.

c. DO/bureaus shall comply with Chapter II, Section 3 of this manual regarding notification requirements when significant adverse information is developed in the case of a DO/bureau contractor that results in a potentially unfavorable determination for access to (1) DO/bureau facilities, (2) sensitive information, or (3) IT/AIS.

Chapter I
Section 4

Personnel Security Operations

Updated
1/3/12

1. Purpose

The purpose of this section is to outline specific procedures to ensure compatibility and consistency in the use and maintenance of personnel security investigations and records. Departmental Offices (DO)/bureaus are responsible for maintaining personnel security operations as specified in this section.

2. Policy

a. DO/bureaus must establish and maintain a personnel security file for employees in the following positions: (1) national security positions, (2) moderate- and high-risk public trust positions, and (3) those in low-risk/non-sensitive positions on whom unfavorable or derogatory information has been developed or received, unless the file is maintained by the Office of Personnel Management (OPM).

b. Contractors are subject to the same requirements as DO/bureau employees with a file maintained for contractor personnel covered by the provisions of Chapter II, Section 2, of this Manual or who require a background investigation to meet the requirements of Homeland Security Presidential Directive (HSPD-12). DO/bureaus need not maintain a file on contractor personnel who was granted access to classified information under the National Industrial Security Program (NISP), unless there is a requirement for additional investigation in connection with (1) access to DO/bureau facilities or automated information systems, or (2) access to classified information (Sensitive Compartmented Information) not covered under the NISP.

c. With regard to favorable investigations on employees or contractor personnel in low- or moderate-risk positions, DO/bureaus may, at their discretion, retain either the entire report or pertinent investigative data only.

d. The specific location of personnel security files is left to DO/bureau discretion, however, all national security files are to be maintained by the DO/bureau security officer.

3. Personnel Security Files

a. *Contents of Personnel Security Files.* Personnel security files include the following documentation:

- The type of investigation completed.
- The investigative agency that conducted the investigation.
- The date of the investigation.
- Results of the investigation.
- Results of security and suitability adjudications/determinations.
- Security clearance decisions.
- Any significant personnel security or suitability information that is developed during employment.

b. *Retention of Personnel Security Files.* Personnel security files should be retained for the duration of an individual's employment or contractual relationship with DO/bureaus and shall be maintained in accordance with Treasury Directive (TD) 80-05, Records and Information Management Program, and National Archives and Records Administration General Records Schedule 18 (items 21-25 relating to personnel security files).

c. *Use of OPM Investigative Reports.* DO/bureaus may choose to retain copies of OPM investigative reports for the duration of the retention schedule; however, OPM Form 79A (*Report of Agency Adjudication Action on OPM Personnel Investigations*) must be retained in the case file as the record of adjudicative action. Reports of investigations conducted by other Federal agencies, but transmitted through OPM, must be handled in the manner prescribed by (1) the originating agency's Privacy Act System Security Notice, or (2) stamped caveats that may appear on those documents.

Disclosure of OPM reports of investigation must be done in a manner consistent with OPM requirements for receipt and distribution of such information. If such disclosure is to the same individual(s) on a recurring basis, those individuals are investigated at the level required by OPM.

d. *Disposition of Investigative Reports.* Personnel security case files and related indices must be destroyed or transferred to a Federal Records Center upon notification of an employee's death, or not later than five years after separation or transfer, or expiration of the contractual relationship. DO/bureaus must ensure that the Privacy Act Notice of Routine Uses for that system of records accurately describes their practices in this area. Investigative reports and related documents obtained from other agencies for making security/suitability determinations must be destroyed in accordance with the investigating agency's instructions.

e. *Compliance with OPM.* DO/bureaus must establish procedures to ensure compliance with OPM's Clearance Verification System (CVS).

4. Security Clearance Records

a. *Certificate of Clearance and/or Security Determination.* Treasury Department Form (TD F) 15-03.2, or bureau equivalent documents the date and basis of the determination, but does not reflect any adverse information recorded in the personnel security file. When a security clearance has been granted, the form should include the level of security clearance granted, and whether it was granted on an interim or final basis.

For employees who do not require security clearances, the form must contain the same biographical and investigative information, but the level of security clearance shall be reflected as "None" or "None Required."

The form must be signed by the personnel security officer or other authorized official, and the signed certificate must be sent to the employee's personnel office. That office shall file original on the right side of the Official Personnel Folder (OPF) with a copy affixed as the uppermost document in the personnel security file.

b. *Classified Information Nondisclosure Agreement* (SF 312*)*. As a condition of being granted access to classified information, the individual must first receive a security briefing by appropriate DO/bureau security officials in which he or she is informed of the obligations and responsibilities attendant upon being granted access, and must execute the SF 312.

(1) For employees, the original SF 312 shall be placed on the right side of the OPF. A copy of the SF 312 may also be retained in the employee's personnel security file.

(2) For individuals not having an OPF, DO/bureaus must maintain the SF 312 in an appropriate system of records that meets the Information Security Oversight Office 50-year retention requirement.

c. *Written Consent Form for Access to Financial Records.* Every employee granted access to classified information must provide the employing DO/bureau with a written consent form. The consent form allows an authorized investigative agency access to financial and other records as defined in Executive Order (EO)

12968 Section 1.2(e), *Access to Classified Information*, for the duration of the employee's access to classified information plus three years thereafter when any of the following occur:

(1) There are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power.

(2) DO or a bureau has received credible information that an employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information.

(3) Circumstances indicate that the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

5. Transfer of Personnel Security Records and Clearances between DO/Bureaus

a. When an employee transfers from DO to a bureau or from one bureau to another, the complete personnel security file or a copy of it must be transferred from the personnel security office of the losing bureau to the personnel security office of the gaining bureau. Exception: when the file of an Internal Revenue Service (IRS) employee contains tax information, the tax information is not transferred outside the IRS.

b. A current security clearance is transferable between DO/bureaus without re-adjudication. DO/bureaus must complete a "Checklist of Permitted Exceptions to Reciprocity" (Attachment 1) prior to requesting additional information, security forms or investigations on employees with existing investigations.

6. Protection of Personnel Security Records

Information in personnel security investigations, records, and operations, must be carefully safeguarded to protect the interests of both the individual and the DO/bureaus as required by the Privacy Act. Personnel security records containing classified information must be stored in a General Services Administration-approved security container or in an equally secure area accessible only by appropriately cleared DO/bureau officials. Personnel security records containing Personally Identifiable Information must be afforded a degree of protection to preclude access by unauthorized persons and be made available and used only for authorized official purposes.

a. Personnel security investigation information requested by the subject of an investigation must be processed according to procedures established by DO/bureaus under provisions of the Privacy Act or the Freedom of Information Act, as appropriate. Requests for the release of the results of any personnel

security investigation should be referred to the DO/bureau or non-Treasury agency that conducted it.

b. Reports containing classified information must be protected in accordance with EO 12958, as amended, *Classified National Security Information*, and appropriate Treasury regulations.

7. Monitoring Personnel, Security Clearance Changes and Adverse Information

a. DO/bureaus shall institute procedures to ensure that all of the following employee information is reported in a timely manner:

- Change of name.
- Marriage or cohabitation.
- Termination of employment.
- Reduction in force.
- Furlough.
- Leave of absence for a period exceeding one year.
- Death of an employee.

b. Any adverse information concerning employees authorized access to or being processed for access to classified information must be reported, when such information becomes known, to the Director, Office of Security Programs or bureau security officer, as appropriate. An individual's failure to report such adverse information to the personnel security official or designated official may result in the suspension or termination of their security clearance. This report must be submitted even if the employment of the individual has been terminated. The report must contain:

- Subject's last, first, and middle name.
- Social security number.
- Date and place of birth.
- Clearance level and date of clearance.
- Employment status (if terminated, include termination date).
- The adverse information being reported.
- The name and telephone number of the individual to contact for further information regarding the matter.
- Signature, typed name, and the title of the individual submitting the report.

c. Reports based on rumor or innuendo shall not be made.

8. Clearance Verification

a. Only the issuing U.S. Government authority may officially verify an employee's security clearance for access to classified information. Within DO this is the responsibility of OSP's Personnel Security Branch. Corresponding bureau security clearance verification is the responsibility of bureau personnel security officials.

b. Passing the clearance includes the level of access the employee has been authorized to receive classified information, e.g., Top Secret, Secret, or Confidential information. Also identified is the type of background investigation conducted, by whom, along with the date the investigation was completed. When an individual's clearance needs to be passed to another Treasury bureau or other U.S. Government agency/department it must be passed from issuing personnel security office to receiving personnel security office.

c. Clearance information shall be passed on DO/bureau letterhead. Employees should notify personnel security officials at least 24 hours before a particular classified meeting or event requiring the clearance to be passed. The OSP website at http://intranet.treas.gov/security/forms/ has Treasury Department Form (TD F) 15-03.6 (Request for Security Clearance Verification), see Attachment 1, and may be used by employees to ask that their clearance be passed. Details regarding the proposed must be provided to the host DO/bureau personnel security office sufficiently in advance of the intended activity to permit timely processing of each request. Details include the following:

- Date(s) of the visit.
- Purpose of the visit.
- Level of the employee's security clearance.
- Name and telephone/fax number of a point of contact at the receiving site.

d. A clearance may be certified to attend routinely scheduled meetings/briefings for up to one year intervals. This saves time and is more efficient than passing a clearance for individual classified meetings. The same rules apply on providing the other agency/department/bureau point of contact information (name, phone/fax number and purpose).

e. When a DO/bureau employee visits a classified facility and that location requires the employee's security clearance information be transferred as a condition of the visit, the visitor's DO/bureau personnel security office must certify to the host security office the necessary security clearance status and other required visit data on the employee. Acceptance of interim security clearances is left to the discretion of the agency whose facility is to be visited.

f. When an employee is detailed to another agency, DO or bureau, it is the responsibility of the sending organization (1) to ensure that the employee meets

all investigative/clearance requirements for the new position, and (2) to grant any security clearance required for access to classified information.

g. When employees of other Federal agencies or cleared contractor facilities require access to classified information at DO/bureau facilities, the sponsoring DO/bureau office must ask the personnel security office to obtain the pertinent security clearance verification data on the visitors (see 8a, above). For Federal employees, the verification data must come directly from the visitor's agency. For contractors, verification must be obtained from the parent company or via the Defense Industrial Security Clearance Office.

9. Interaction with Offices of Inspectors General

Personnel security cases and investigations in which evidence of criminal activity is developed shall be referred to the Office of Inspector General, the Office of Inspector General for Tax Administration, or the Office of the Special Inspector General for the Troubled Asset Relief Program, as appropriate.

Attachment 1

Department of the Treasury
Request for Security Clearance Verification

For security clearance information to be verified (passed) as expeditiously as possible, the following data must be provided to Departmental Offices/bureau personnel security specialists holding your clearance certification.

Employee Name: _____ Date of Request: _____

Date of Birth: _____ SSN: _____ Office Phone: _____

Bureau/Agency/Department requiring security clearance verification; phone/fax:

_____

Point of Contact/Sponsor Name: _____

Contact/Sponsor's Phone and Fax Numbers: _____

Meeting/Visit Dates: (from) _____ (to) _____ Permanent Certification Yes No

Location(s) (as applicable): _____

Purpose: _____

_____

Please allow 24 hours from personnel security specialists' receipt of this form for security clearance information to be passed to recipient(s).

Notice: In compliance with the Privacy Act of 1974, 5 U.S.C. § 552a the authority for soliciting your Social Security Number (SSN) is Executive Order 9397 which authorizes agencies to solicit SSNs for use as identifiers for administrative purposes. Your SSN is needed to keep records accurate, because other people may have the same name and birth date. This information will be used as a means of verifying your security clearance to Treasury bureaus and other agencies/departments. Information will be transferred to appropriate Federal, State, local or foreign agencies when relevant to civil, criminal, or regulatory investigations or prosecutions; or pursuant to a request any other agency in connection with hiring or retention of an employee, the issuance of a security clearance, the investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit. Disclosure of the information is voluntary. If some or any part of the requested information is not provided, the effect will be that the processing of your request for security clearance verification will be impeded or possibly result in the denial of access to classified information.

TD F 15-03.6

Chapter I
Section 5

Suspension of Access to Classified Information

Updated
1/3/12

1. Introduction

This section presents the procedures to be followed when suspending an individual's access to classified information, in accordance with Executive Order (EO) 12968. The procedures described herein do not apply to termination of access when the individual no longer has a need-to-know.

2. Suspension of Access to Classified Information for Cause

When questionable or unfavorable information becomes available concerning an individual who has been granted access, the Director, Office of Security Programs (OSP), or Departmental Offices (DO)/bureau personnel security officer, as appropriate, may immediately suspend access. Suspension of access for cause may only be used as an interim measure that must be resolved through either a favorable or unfavorable security determination by the Director, OSP, or DO/bureau personnel security officer, as appropriate. The supervisor will forward all pertinent information concerning the individual to the Director, OSP, or DO/bureau personnel security officer, as appropriate, for a final security clearance determination.

Suspension of access is required when an individual with a security clearance is incarcerated (to include Work Release Programs) as the result of a conviction for a criminal offense or is absent without leave for a period exceeding 30 days.

Suspension of access may be appropriate in, but not limited to, any of the following situations:

(1) Preparations are being made to revoke an individual's existing security clearance and access is suspended while the review of the determination to revoke takes place.

(2) Additional time is needed to resolve adverse information that could require further investigation or the individual must complete certain requirements to maintain his or her eligibility to maintain a security clearance.

(3) Pending removal and termination of employment resulting from adverse personnel actions under 5 United States Code 75.

(4) Failure by an individual to submit required security forms or releases in a timely manner.

Whenever a determination is made to suspend access to classified information, the following will occur:

- The individual concerned will be notified in writing of his/her suspended access to classified information by the Director, OSP, or DO/bureau personnel security officer, as appropriate, consistent with the interests of national security. Notification to an individual regarding suspension of access to classified information may be by personal delivery, government or commercial overnight carrier, or certified mail. It must be delivered in a timely manner and an acknowledgment of receipt shall be requested. Regardless of whether delivery of the notice to the individual is refused or does not reach the individual through no fault of the Director, OSP or DO/bureau personnel security officer, suspension of access to classified information is immediate.

- A copy of any notification required by this section shall be maintained in the individual's personnel security file and a copy shall be provided to the Director, OSP.

- A brief statement of the reason(s) for the proposed suspension will be included.

- The suspension of access to classified information remains in effect until an appropriate investigation is conducted and/or a determination is made to revoke or reinstate an individual's access to classified information by the Director, OSP or DO/bureau personnel security officer.

Upon the suspension of an individual's access to classified information:

- The Director, OSP, or DO/bureau personnel security officer, as appropriate, in conjunction with the individual's supervisor, will take steps to ensure that the individual's name is removed from all access rosters, and notice of visit certifications provided to other agencies. Additionally, all employees (including contractors) working with the affected individual must be notified of the suspension (without disclosing the cause of the suspension) to ensure the individual has no further access to classified information.

- Combinations to classified storage containers (safes) to which the individual had access will be changed unless sufficient controls exist to prevent the individual's continued access to the security container.

- The Director, OSP, DO/bureau personnel security officer, and/or the individual's supervisor, as appropriate, will ensure that the individual does not have access to any classified information during the period of the suspension of access to classified information.

Chapter I Section 6 **Denial or Revocation of Security Clearance** Updated 1/3/12

1. Introduction

This section presents the procedures to be followed when denying or revoking an employee's security clearance, in accordance with Executive Order (EO) 12968, *Access to Classified Information.* The process to appeal a decision is presented in Chapter I, Section 7.

The procedures in this section are applicable except where the Secretary of the Treasury invokes the provisions set forth in EO 12968, Section 5.2(c) or (e).

2. Notices and Due Dates

a. Notification to an employee or applicant regarding denial or revocation of security clearance may be sent by personal delivery, government or commercial overnight courier, or certified mail. It must be delivered in a timely manner and an acknowledgment of receipt shall be requested. A copy of any notification required by this section shall be maintained in the individual's personnel security file and a copy shall be provided to the Director, Office of Security Programs (OSP).

b. Unless explicitly stated otherwise, the time period for a reply or other filing by an applicant or employee begins upon delivery of notification to the individual. Where delivery cannot be made or the delivery is refused, the time period begins five calendar days after issuance of notification to the individual.

The due date specified for a reply or other filing by an individual is the date the reply or other filing must be received by the appropriate Departmental Offices (DO)/bureau office. The reply or other filing can be made by personal delivery, facsimile, mail, or GSA-approved commercial overnight delivery.

3. Denial or Revocation of Security Clearance

DO/bureaus should proceed with denial or revocation, as appropriate, when the responsible DO or bureau personnel security officer determines either of the following:

a. An individual who has been nominated for or currently possesses a security clearance fails to meet applicable security criteria.

b. There are insufficient mitigating factors indicating whether security clearance eligibility may be granted in the future.

4. Notification of Determination

The individual must be provided with the review proceedings below as set forth in Section 5.2, EO 12968.

The applicant or employee must be provided with a written notice of determination stating that he or she does not meet applicable eligibility standards for access to classified information. The written notice of determination must contain the following information:

a. As comprehensive and detailed an explanation of the basis for the determination as the national security interests and other applicable laws permit.

b. The name and address of the official to whom the employee should direct any reply, request, or other filing.

c. A copy of this section of the Treasury Security Manual (Chapter I, Section 6) and a statement directing the individual to this section for a description of the review proceedings available to him or her.

d. A copy of EO 12968.

5. Review of Determination

a. If an individual to whom a notice of determination is issued requests a review of the determination, he or she may:

(1) Be represented by counsel or other representative at their own expense.

(2) Request, in writing, not later than 15 (fifteen) days after receipt of the Notice of Determination, either or both of the following:

- Any documents, records, and reports upon which a denial or revocation is based, as defined in section 5.2(a)(2) of EO 12968.

- The entire investigative file, as permitted by the national security and other applicable laws.

(3) Request, in writing, a review of that determination, within the following timeframes:

- No later than 30 (thirty) days after receipt of the Notice of Determination, if no timely request has been made under paragraph 5a (1) above.

- No later than 30 (thirty) days after receipt of a notice from DO/bureau to the individual that the DO/bureau has made the final release of material requested, where a timely request under paragraph 5a (2), above, has been made.

(4) Request to appear personally before the deciding authority (the DO/bureau official designated to review any reply to the notice of determination), and present relevant documents, materials, and information. A request to appear personally shall be made no later than the time at which a written reply to a notice of determination would be timely made.

b. DO/bureaus must notify the individual when final release of documents or the file is made, so that the due date for a written reply may be set.

(1) If the applicant or employee requests any documents, records, or reports upon which a denial or revocation is based, the documents must be provided to the individual within 30 days of receipt of the request. The documents must be provided to the extent they would be provided if requested and released under the Freedom of Information Act or the Privacy Act, as applicable.

(2) If the applicant or employee requests the entire investigative file, such documents must be provided promptly prior to the time set for a written reply, as permitted by the national security and other applicable law.

c. A reply to the notice of determination must be reviewed by an official designated by DO/bureau officials or personnel security authority.

Note: The deciding authority shall not be under the supervision of the individual issuing the notice of determination.

(1) If the applicant or employee timely requests an opportunity to appear personally, the deciding authority must comply with the provisions of Section 5.2(a)(7), EO 12968, be present at the personal appearance, and prepare a written summary or recording of the personal appearance, at DO/bureau discretion. The deciding authority will also make any necessary rulings for the conduct of the personal appearance and regulate the proceeding as may be necessary.

Note: A confrontation interview as part of the investigation does not constitute an opportunity to appear personally.

(2) Upon completion of the review of the case, the deciding authority must notify the individual in writing of his or her decision (referred to as a Notice of Review). In the Notice of Review, the deciding authority must state the reasons for the decision.

If the decision of the deciding authority affirms the determination to deny or revoke the security clearance, the Notice of Review must also inform the individual of the right to appeal the decision to the Treasury Department's Security Appeals Panel, as described in Section 5.2(a)(7), EO 12968,

To file an appeal, the individual must submit a written appeal to the Security Appeals Panel at the following address, within 30 days of receipt of the Notice of Review:

Security Appeals Panel
c/o Director, Office of Security Programs
Room 3180 Treasury Annex
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20220

d. Appeals are decided by the Treasury Department's Security Appeals Panel, which is discussed more fully in Chapter I, Section 7.

6. Final Action

a. When an applicant or employee timely requests a review of a notice of determination or, after such review, appeals to the Security Appeals Panel, the denial or revocation of eligibility for access to classified information is implemented only when any or all such proceedings have been completed.

b. Failure of the applicant or employee to (1) request review of the determination, (2) appeal to the Security Appeals Panel, or (3) meet any applicable time limit for these actions normally results in the termination of any further proceedings. The denial or revocation of security clearance is implemented at that time.

7. Responsibilities for Rulings

a. Until a deciding authority is designated, the official who issues the notice of determination will make any necessary rulings with respect to these proceedings. Upon designation of the deciding authority, the deciding authority will make any necessary rulings on these proceedings.

b. Upon receipt of a written appeal to the Security Appeals Panel, the Chair of the Panel shall make any necessary rulings on procedural matters.

8. No Rights Created

These provisions, consistent with Section 5.2 (c), EO 12968, create no procedural or substantive rights.

Chapter I
Section 7

Security Appeals Panel Procedures

Updated
1/3/12

1. Introduction

This section outlines the procedures for the appeal of a security clearance denial or revocation, including the responsibilities of the Department of the Treasury Security Appeals Panel, in accordance with Executive Order (EO) 12968, *Access to Classified Information,* Part 5, Review of Access Determinations. The appeal process is available to all Departmental Offices (DO)/bureau employees who have been determined to be ineligible for access to classified information.

Denial and revocation of eligibility for a security clearance can have a severe impact on an individual and their career; therefore, the reconsideration and appeals procedures must be carefully followed to ensure that both security and fairness requirements are met.

2. Notice of Review

Upon completion of the review of a case, the deciding authority must notify the employee in writing (via *Notice of Review*) of the deciding authority's decision, the reasons for the decision, and identify the deciding authority.

3. Appeal of the Determination

Appeals are resolved by the Treasury Department's Security Appeals Panel, which is appointed by the Deputy Assistant Secretary for Security. The panel includes at least two persons from outside the security field. The Director, Office of Security Programs shall be a member and chair of the Security Appeals Panel. Upon request of the Security Appeals Panel, all relevant case materials will be provided by the deciding authority, including the written summary or recording of any personal appearance.

If the panel determines that additional information or investigation is necessary to render a decision, the chair may request such information or investigation from the DO/bureau where the case originated.

The Secretary of the Treasury may personally certify that the appeals process cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information. In such cases, the appeals process shall not be made available. This certification shall be conclusive.

4. Notice of Right to Appeal

The written notice of the results of a review must contain the following statement:

> You have the right to appeal this determination to the Treasury Department 's Security Appeals Panel within 30 days of your receipt of this notice. Your appeal should be addressed to:
>
> Security Appeals Panel
> c/o Director, Office of Security Programs
> Room 3180 Treasury Annex
> 1500 Pennsylvania Avenue, N.W.
> Washington, D.C. 20220

The appeal must be in writing and must contain the following information:

- Your full name, address and telephone number(s).
- The name, address and telephone number of your attorney or other representative, if any.
- A copy of this notice.
- Any written statement, relevant documents, materials, or information you wish the Security Appeals Panel to consider.

Note: Classified national security information involved in the appeals process must be protected. Access to this information may only be granted pursuant to the requirements set forth in EO 12968.

5. Timeliness of Appeal

An appeal filed outside the 30-day time limit will not be accepted by the Security Appeals Panel unless the appellant demonstrates compelling reasons beyond his or her control that prevented timely filing. Failure of the applicant or employee to request an appeal within the required time limit will result in a termination of any further proceedings. The denial or revocation of security clearance shall be upheld at that time.

6. Supplementary Information

If the panel determines that additional information or investigation is necessary to render a decision, the Chair of the Security Appeals Panel may request such information or investigation from the DO/bureau wherein the case originated. The DO/bureau shall ensure that the request is fulfilled.

7. Personal Appearance Before Panel

The appellant has the right to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority. This opportunity will be exercised at the bureau level. The Security Appeals Panel may, at their discretion, afford the appellant the opportunity to appear before them.

a. *Recording*. The Security Appeals Panel determines whether and how the personal appearance will be recorded and transcribed. No other mechanical recording of the personal appearance will be permitted.

b. *Attendance*. Only the appellant, the appellant's representative, the Security Appeals Panel members, and a representative from the Treasury Legal Counsel are permitted to attend the appellant's personal appearance.

c. *Informal Proceeding*. Because the personal appearance is an informal proceeding, statements will not be made under oath. There will be no right to present of cross-examine witnesses.

8. Decision

The decision of the Security Appeals Panel shall be in writing and is final unless the Secretary of the Treasury personally exercises appeal authority based upon recommendations from the Security Appeals Panel. In such case, the decision of the Secretary shall be final.

The Security Appeals Panel shall provide its decision in writing to the appellant or the appellant's representative with a copy to the DO/bureau.

Chapter I Section 8

Presidential Policy Directive 19, Protecting Whistleblowers with Access to Classified Information

Dated 6/21/13

1. Introduction

Treasury employees are protected by the Whistleblower Protection Act of 1989. Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information,* dated October 10, 2012 further ensures that employees, serving in the Executive Branch, who are eligible for access to classified information, can effectively report waste, fraud, and abuse while protecting classified national security information and prohibits retaliation against employees for reporting such waste, fraud and abuse.

Any DO/bureau official who has authority to take, direct others to take, recommend or approve any action affecting an employee's eligibility for access to classified information, shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take any action affecting an employee's eligibility for access to classified information as a reprisal for a protected disclosure.

2. Protected Disclosure

PPD-19 applies to the protected disclosure" of information, i.e., disclosure of information by an employee to a supervisor in the employee's direct line of authority up to and including the DO/bureau head, to the Inspector General of the employing DO/bureau (collectively "Inspector General"), or to an employee designated by any of the above officials for the purpose of receiving such disclosures, that the employee reasonably believes evidence (1) a violation of any law, rule, or regulation; or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. The term "protected disclosure" includes:

a. Any communication described by and that complies with subsection (a)(1), (d), or (h) of section 8H of the Inspector General Act of 1978; subsection (d)(5)(A) of section 17 of the Central Intelligence Agency Act of 1949; or subsection (k)(5)(A), (D), or (G) of section 103H of the National Security Act of 1947;

b. The exercise of any appeal, complaint, or grievance with regard to the violation of PPD-19;

c. Lawfully participating in an investigation or proceeding regarding a violation of PPD-19; and

d. Cooperating with or disclosing information to an Inspector General, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General, if any of the actions in (paragraph 2b-d above) do not result in the employee disclosing classified information or other information contrary to law.

3. Review Process

Employees may appeal actions they allege to be in violation of PPD 19 as grounds for the review of eligibility decisions described in Sections 6 and 7 of this Chapter. If adequate review requires the disclosure of classified information, the employee shall contact the appropriate DO/bureau official or the Director, Office of Security Programs (OSP), to make the necessary arrangements.

If an employee alleges a violation of PPD-19 during the processes described in Sections 6 and 7 of this Chapter, the matter shall be referred to the relevant Inspector General by the Director, OSP, upon exhaustion of the employee's review or appeal rights, for the Inspector General's review to determine whether an action affecting eligibility for access to classified information violated PPD-19. The Inspector General may recommend to the last reviewing official or panel appropriate corrective action. That official or panel shall carefully consider the findings of and actions recommended by the Inspector General for reconsideration of the employee's eligibility for access to classified information consistent with EO 12968 and may amend its review determination. To the extent authorized by law (including the Back Pay Act), such action may include, but is not limited to, reinstatement, reassignment, the award of reasonable attorney's fees, other reasonable costs, back pay and related benefits, travel expenses, and compensatory damages.

4. Appeal Process by External Panel Review

An employee alleging reprisal in violation of PPD-19 who has exhausted the review processes described in Sections 6, 7, and 8.4 of this Chapter may request an external review by a three-member Inspector General panel as required by Section C of PPD-19 by notifying the Inspector General of the employing DO/bureau. PPD-19 requires the external panel to complete a review of the claim, which may consist of a file review, as appropriate, within 180 days.

If the external panel determines the individual was subject to an action affecting his or her eligibility for access to classified information based upon reprisal, it may recommend that the last reviewing official or panel take corrective action to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred and that the official or panel reconsider the employee's eligibility for access to classified information consistent with the national security and EO 12968.

The last reviewing official or panel head shall carefully consider the recommendation of the external panel and within 60 days inform the employing DO/bureau and the Director, OSP, of its determination with respect to the recommendation. The Director, OSP, shall within 90 days, ensure that the external panel and the Director of National Intelligence are informed of what action has been taken.

Chapter II
Section 1

Personnel Security and Suitability Investigations

Updated
12/1/11

1. Introduction

The purpose of this section is to present the minimum requirements and standards within the Department of the Treasury to determine whether an individual's employment promotes the efficiency of the service (suitability) and is consistent with the interests of the national security, as set forth in Title 5 Code of Federal Regulations 731 and 732, respectively.

Senior managers, supervisors, and employees are responsible for familiarization and compliance with all personnel security regulations and procedures at their installations.

2. Policy

Every position within Departmental Offices (DO)/bureaus requires that incumbent employees undergo an investigation conducted by an appropriate government authority based upon the (1) requirements of Homeland Security Presidential Directive (HSPD-12), (2) sensitivity of the position, and/or (3) need for access to classified information. The investigative requirements shall be consistent with the guidance provided by the Office of Personnel Management (OPM).

3. Personnel Security Program

a. The objective of the Personnel Security Program is to authorize initial and continued access to classified information and/or initial and continued assignment to sensitive duties. The program applies to those persons whose loyalty, reliability and trustworthiness are such that entrusting the persons with classified information or assigning the persons to sensitive duties is clearly consistent with the interests of national security.

b. The policies, procedures, and standards prescribed in this section apply to DO/bureau employees and applicants as well as individuals working as consultants or experts, students, trainees, and other persons designated by the Secretary of the Treasury to have access to classified information or assigned to sensitive duties.

4. Investigative Responsibilities

By agreement with the OPM Federal Investigative Services Division (OPM-FISD), and subject to special agreements between OPM- FISD, the DO/bureau background investigative responsibility is divided as follows:

a. On a reimbursable basis, OPM-FIS will conduct standard suitability and national security investigations as requested by DO/bureaus pursuant to a written agreement between OPM-FISD and DO/bureaus. In addition to general agreements, DO/bureaus may enter into special agreements with OPM-FISD to have OPM-FISD provide other investigative services on a reimbursable basis. The duration of special agreements and the timing for notice to amend or cancel them will be established at the time that the agreements are prepared.

b. DO/bureaus with delegated investigative authority may conduct investigations where special agreements have been made with OPM-FISD, including all or part of the National Agency Check (NAC), as well as such additional investigation, as necessary, to resolve unfavorable or inconsistent information developed during the background investigation. DO/bureaus with delegated authority must conduct investigations for competitive service applicants, appointees, and employees that meet the investigative standards set by OPM-FIS, as covered in the OPM Investigator's Handbook.

c. In order to obtain investigative authority, DO/bureaus must first submit a business/operations plan to the Director, OSP. The Director, OSP will evaluate the plan and forward his/her recommendation to OPM-FISD. The DO/bureau business/operations plan must contain the following information:

(1) Type of investigators DO/bureaus will employ (government employees, independent contract employees or contract investigation companies.)

(2) Training plan DO/bureaus will utilize to train investigators and internal review staff.

(3) Quality Assurance plan DO/bureaus will utilize to monitor:

a. Investigators interviewing techniques, report writing skills and professionalism while conducting interviews.

b. Internal review staff proficiency in evaluating completed investigations against national investigative standards for completeness and issue resolution.

(4) Description of information technology/ automated information system(s) to be utilized in tracking

a. investigative leads assignments to investigators.

b. timeliness of investigative leads.

(5) Signed memoranda of agreement with appropriate Federal agencies if DO/bureaus intend to conduct any portion of the NAC.

d. OSP reserves the authority to conduct period reviews of all DO/bureaus investigation programs.

5. Suitability and Security Investigations

a. Suitability and security investigations:

(1) Provide an assessment of an individual's potential likelihood to promote the efficiency and integrity of DO/bureau operations when filling a particular position.

(2) Determine if employment or retention in employment is consistent with the national security.

b. The investigative process for both types of investigations develops information and evaluates the background of employees associated with the Department. The findings of facts ascertained through security investigations are used to determine eligibility for access to national security information or for special access program determinations. General guidance showing the minimum type of security and suitability investigation for each sensitivity or risk level is provided in Chapter I, Section 1.

c. Employees appointed to any DO/bureau position are subject to a suitability investigation (1) upon initial appointment to the Federal service and (2) upon reappointment after a break in service of 24 or more months. Employees also may be subjected to investigation for access to national security information prior to or immediately following entrance-on-duty, in accordance with the provisions of the Treasury Security Manual (TD P 15-71). Current Federal employees appointed to DO/bureau positions may be subjected to further investigation, if the position to which they are being appointed carries a higher risk designation than that for which they were previously investigated. In general, the type of investigation to be conducted is based on the position's sensitivity or risk level designation.

d. All non-employees, such as persons working under personal contracts i.e., consultants or experts, are subject to investigation under guidelines set forth in Homeland Security Presidential Directive 12 (HSPD-12) if they have an official association with an operating unit or office. In general, the type of investigation to be conducted is based on the risk associated with the individual's work and the anticipated period of association with DO/bureau.

6. Initiating Requests for Investigations

Investigations are initiated for several reasons.

a. Every employee shall undergo a suitability investigation prior to or immediately following entrance-on-duty. A suitability investigation shall be initiated upon selection of an individual for employment within the DO/bureau.

The immediate supervisor or human resources officer must request a suitability investigation for the new employee.

(1) For all positions designated Low Risk, the Standard Form 85 (SF 85) is used. For positions designated Moderate or High Risk, the SF 85P is used. The SF 85P-S is used only after obtaining written approval of OPM.

(2). The DO/bureau security office directs the applicant to either submit the required information via OPM's Electronic Questionnaire for Investigations Processing (OPM's e-QIP) or on paper via an SF 85 or SF 85P. The SF 85 or SF 85P provides current biographical information to allow for an investigation to establish eligibility for access.

b. Although position sensitivity may dictate a more detailed investigation, the following security clearance levels require the minimum types of investigation indicated below:

(1) *Top Secret.* A Single Scope Background Investigation (SSBI) no more than five years old, or updated by a Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR) within the most recent five-year period.

(2) *Secret.* An Access National Agency Check and Inquiries (ANACI) no more than ten years old and no break in Federal service of greater than 23 months.

Prior to movement to a new position that requires access to classified information or when the assignment results in a significant change in duties, a request for security clearance must be forwarded to the appropriate DO/bureau personnel security office or component for approval, even if the assignment involves the same level of security clearance as the employee's current position.

(1) When an employee occupies a position that subsequently requires access to classified information, the employee may continue to perform in the position provided access to classified information is prevented until the responsible DO/bureau security office grants the appropriate security clearance. Background investigations are initiated within 14 days of the effective date of the new position designation.

(2) When an employee moves to a position that requires access to a higher level of classified information, the employee may continue to perform in the position and have access to classified information at the level for which he or she has previously been granted until the responsible DO/bureau personnel security office upgrades the security clearance to the higher level clearance or grants the appropriate level of temporary or interim access. Background investigations will be initiated within 14 days of the effective date of the new position designation.

c. Investigations are initiated via e-mail or other written request. The immediate supervisor or program manager requests and justifies a security clearance for a subordinate employee. The request is forwarded to the appropriate DO/bureau personnel security office.

(1) The request states the level of clearance (*Top Secret, Secret* or *Confidential*) and justifies the request for access. The request describes the individual's "need-to-know," the nature of access, how often it will occur, and the duration required for the security clearance. If the duration is indefinite, it must be so stated.

(2) The DO/bureau personnel security office will direct the applicant to either submit the required information via OPM's E-QIP or on paper via a SF 86, *Questionnaire for National Security Positions*. A new or updated SF 86 is required when the security office does not have one on file.

Note: The SF 86 provides current biographical information to allow an investigation to establish eligibility for access.

(3) SF 312, *Classified Information Nondisclosure Agreement*, can only be signed after eligibility for access to classified information has been granted by the approving authority; therefore, it will not be executed and sent with the clearance request package.

(4) The individual must sign SF 312 immediately after receiving the required security indoctrination briefing since it is a legally binding document that grants the signer eligibility for access to classified information upon signature in return for abiding by its requirements.

(5) The supervisors and managers requesting a security clearance for a subordinate employee are responsible for following the safeguarding requirements and procedures described in Chapters III and V.

7. Investigative Scope

Investigative scope and standards applicable to each level and category of classified information were established by the former Security Policy Board, approved by the President, and are still in use. Investigative requirements of sensitive positions are established by OPM.

Nothing in this section shall prevent DO/bureaus from establishing additional requirements that may be necessitated by mission responsibilities. However, investigations for access to classified information must be in compliance with Executive Order (EO) 12968 or any other EO, regulation, or statute pertaining to granting access to classified information.

a. *Periodic Reinvestigations are Mandatory.* Circumstances and characteristics may change dramatically over time and thereby alter the eligibility of an employee's continued access to classified information. Periodic reinvestigations shall be conducted with the same priority and care as initial investigations. The timeframes for reinvestigation are as follows:

(1) All personnel with access to classified information must be reinvestigated periodically, according to clearance level.

- Personnel with access to *Top Secret*, "Q", and SCI will be reinvestigated at least every five years.
- Personnel with a *Secret* or "L" clearance will be reinvestigated at least every ten years.
- Personnel with a *Confidential* clearance will be reinvestigated at least every 15 years.

(2) Personnel with no access to classified information, that is, personnel in positions designated Critical-Sensitive, High Risk, and those in Law Enforcement or Public Trust positions that are designated Moderate Risk, are subject to a Periodic Reinvestigation (PRI) no later than five years after placement and at least once every succeeding five years.

b. If there is a change in position risk or sensitivity level, i.e., an employee moving to a position at a higher risk or sensitivity level than the position he or she currently occupies, the employee must meet the investigative requirements of the position designation of the new position.

(1) For an employee moving into a *Critical-Sensitive* or *Special-Sensitive* position, the investigation must be completed pre-appointment (reference Part 8 for waiver conditions).

(2) Other than for *Special* or *Critical-Sensitive* levels, if the position risk or

sensitivity of an incumbent's position is increased due to an accretion of duties and responsibilities, the incumbent may remain in the position, but the investigation required by the higher risk/sensitivity level should be initiated within 14 working days of the effective date of the new position designation.

(3) Movement of an employee into a *Special-Sensitive* position must be made in consultation with the Director, Office of Security Programs (OSP).

8. Waivers of Pre-appointment Investigations

In accordance with EO 10450, Section 3(b), and 5 CFR 732, at a minimum, a request for a waiver of a required pre-appointment investigation for *Critical-Sensitive* positions shall be based on the existence of the following:

- The nature of the emergency and/or critical need requiring immediate appointment precludes obtaining pre-waiver checks.
- Checks were initiated but not all responses were received within five days.
- Checks made and favorably completed are listed.

Waiver requests must be submitted to the Director, OSP for approval. The requirement for pre-appointment investigation for *Special-Sensitive* positions may not be waived.

9. Credit Checks

In accordance with the Fair Credit Reporting Act, all DO/bureau applicants and employees, including contractor employees, for whom a credit check is initiated, will be notified in writing that credit reports may be obtained for employment purposes. Written consent must be obtained prior to any such reports being procured. Individuals must be notified promptly if information in their credit report may result in any unfavorable action, such as denial of a clearance, employment, or access authorization. TD F 15-03.9, Fair Credit Reporting Act Disclosure and Authorization Form shall be used for this purpose. (See Attachment 1).

10. Other Types of Background Investigations

There are other types of background investigations that are required depending upon the position and circumstances of the individuals for which these investigations must be done.

a. *Child Care Worker Criminal Background Checks.* Public Law 101-647, Child Care Worker Employee Background Checks (42 U.S.C. 13041), requires that (1) each agency of the Federal Government and (2) every facility operated by

the Federal Government (or operated under contract with the Federal Government) that hires (or contracts for hire) individuals to provide child care services to children under the age of 18, shall assure that all existing and newly hired employees undergo a criminal history background check, the results of which shall be communicated to the employing agency. The approved level of investigation is the Child Care National Agency Check with Inquiries (CNACI), which can be procured from OPM.

b. *Investigations for Foreign Governments.* Agencies that conduct background investigations, including the Federal Bureau of Investigation (FBI) and the Department of State, are authorized to conduct personnel security investigations in the United States when a foreign government requests them as part of its own personnel security program and with the consent of the individual.

c. DO/*bureau Employees Assigned/Working Outside the United States.* DO/bureau employees assigned overseas to diplomatic posts/facilities are investigated and clearances issued by the employing DO/bureau personnel security office. On-location part-time, intermittent or temporary (PIT) employees may be hired to work by the Department of State. If the subject is employed by the Department of State (DOS), even if working in a DO/bureau office, the DOS has the responsibility for investigating and granting the security clearance. Consult the State Department's Foreign Affairs Manual (3 FAM 123) for specific steps to follow.

d. *Treasury Advisory Committee Members.* Personnel security procedures relating to participants on advisory committees (1) require that pre-appointment and annual tax checks be requested by sponsoring officials; and (2) include FBI Name Checks and a security clearance.

(1) In order to conduct those inquiries, committee-sponsoring officials are responsible for obtaining the following biographical data from nominees and providing it to the Director, OSP:

- Full Name (last, first and middle).
- Other Names, Aliases, Maiden Names, Pseudonyms Used.
- Date and Place of Birth.
- Social Security Number (SSN).
- Current Home Address.
- Current Employment Address.
- Occupation.

(2) Sponsoring officials shall inform selected advisory commission members of the purpose for requesting the information, as required by the Privacy Act, and that the SSN is used in this instance as an identifier to distinguish between individuals with identical names and birth dates. Sponsoring officials shall obtain a signed tax check waiver, TD F 15-03.10, Tax

Check/Tax Audit Waiver Form from the selected member (See Attachment 3).

(3) When results of the checks are obtained and are favorable, the requesting office is informed that there is no objection to the person participating in the requested capacity. This does not, however, constitute a security clearance for access to classified information.

11. Exceptions to Investigative Requirements

In accordance with 5 CFR 732, sensitive positions that are intermittent, seasonal, on per diem, or temporary and do not exceed an aggregate of 180 days, are exempt from the investigative requirements of EO 10450. However, these sensitive positions are subject to checks deemed appropriate to ensure that the employment or retention of individuals in these positions is clearly consistent with the interests of national security. Individuals performing in intermittent, seasonal, per diem, or temporary positions shall, at a minimum, have a FBI fingerprint and name check. DO/bureaus may require additional investigative efforts as required to meet specific needs.

12. Investigative Requirements after Breaks in Service

If a person who requires access has been retired or separated from U.S. Government employment for less than 24 months and is the subject of an investigation that is otherwise current, the agency granting the access, at a minimum must review an updated SF 86 and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of EO 12968.

Attachment 1

Department of the Treasury
Fair Credit Reporting Act
Disclosure and Authorization Form

This is a release for the Department of the Treasury to obtain one or more consumer/credit reports about you for an investigation in connection with your application for employment or in the course of your employment with the _____/ Department of the Treasury, including your employment as a contractor. One or more reports about you may be obtained for employment purposes, including evaluating your suitability for employment, promotion or reassignment which results in a change to your position risk level, or access to classified information.

I, _____, hereby authorize the Department of the Treasury to obtain such report(s) from any consumer/credit reporting agency for employment purposes. This authorization is valid for 5 years from the signed date, or upon the termination of my employment with _____/ Department of the Treasury, or until the investigation has been completed, whichever is sooner. If I apply for another position that requires a credit inquiry, I understand that I will be required to complete a new authorization. Copies of this authorization that show my signature are as valid as the original signed by me.

_____
Signature

_____
Date

This form is in compliance with the Privacy Act of 1974. Our authorized right to ask for this information is 5 U.S.C. 301 and Executive Order 10450, which established the criteria for sensitive Government positions. The information you supply by signing this release of information form will be used principally to aid in the completion of an investigation to determine your suitability for employment in the Federal service or for other employment purposes. Such purposes include, but are not limited to, a security clearance, evaluation of qualification, suitability, loyalty to the United States, eligibility for access to government information, facilities, or information technology systems, or congressional inquiries. The information obtained may be re-disclosed to other Federal agencies for the above purposes and to the extent that is authorized by law.

Your signature on this release is voluntary, however, your failure to complete this form may mean that the required information cannot be obtained to complete your investigation. This may affect your placement or security clearance prospects.

If the Department of the Treasury intends to take any adverse action based in whole or in part on your credit report, you are entitled to certain protections set out in the Fair Credit Reporting Act, 15 U.S.C. 1681b. These protections are shown on the reverse side of the form.

TD F 15-03.9

A Summary of Your Rights Under the Fair Credit Reporting Act

The federal Fair Credit Reporting Act (FCRA) is designed to promote accuracy, fairness, and privacy of information in the files of every "consumer reporting agency" (CRA). Most CRAs are credit bureaus that gather and sell information about you -- such as if you pay your bills on time or have filed bankruptcy -- to creditors, employers, landlords, and other businesses. You can find the complete text of the FCRA, 15 U.S.C. §§1681-1681u. The FCRA gives you specific rights, as outlined below. You may have additional rights under state law. You may contact a state or local consumer protection agency or a state attorney general to learn those rights.

You must be told if information in your file has been used against you. Anyone who uses information from a CRA to take action against you -- such as denying an application for credit, insurance, or employment -- must tell you, and give you the name, address, and phone number of the CRA that provided the consumer report. **You can find out what is in your file.** At your request, a CRA must give you the information in your file, and a list of everyone who has requested it recently. There is no charge for the report if a person has taken action against you because of information supplied by the CRA, if you request the report within 60 days of receiving notice of the action. You also are entitled to one free report every twelve months upon request if you certify that (1) you are unemployed and plan to seek employment within 60 days, (2) you are on welfare, or (3) your report is inaccurate due to fraud. Otherwise, a CRA may charge you up to eight dollars. **You can dispute inaccurate information with the CRA.** If you tell a CRA that your file contains inaccurate information, the CRA must investigate the items (usually within 30 days) by presenting to its information source all relevant evidence you submit, unless your dispute is frivolous. The source must review your evidence and report its findings to the CRA. (The source also must advise national CRAs -- to which it has provided the data -- of any error.) The CRA must give you a written report of the investigation and a copy of your report if the investigation results in any change. If the CRA's investigation does not resolve the dispute, you may add a brief statement to your file. The CRA must normally include a summary of your statement in future reports. If an item is deleted or a dispute statement is filed, you may ask that anyone who has recently received your report be notified of the change. **Inaccurate information must be corrected or deleted.** A CRA must remove or correct inaccurate or unverified information from its files, usually within 30 days after you dispute it. **However, the CRA is not required to remove accurate data from your file unless it is outdated (as described below) or cannot be verified.** If your dispute results in any change to your report, the CRA cannot reinsert into your file a disputed item unless the information source verifies its accuracy and completeness. In addition, the CRA must give you a written notice telling you it has reinserted the item. The notice must include the name, address and phone number of the information source. **You can dispute inaccurate items with the source of the information.** If you tell anyone -- such as a creditor who reports to a CRA -- that you dispute an item, they may not then report the information to a CRA without including a notice of your dispute. In addition, once you've notified the source of the error in writing, it may not continue to report the information if it is, in fact, an error. **Outdated information may not be reported.** In most cases, a CRA may not report negative information that is more than seven years old; ten years for bankruptcies. **Access to your file is limited.** A CRA may provide information about you only to people with a need recognized by the FCRA -- usually to consider an application with a creditor, insurer, employer, landlord, or other business. **Your consent is required for reports that are provided to employers, or reports that contain medical information.** A CRA may not give out information about you to your employer, or prospective employer, without your written consent. A CRA may not report medical information about you to creditors, insurers, or employers without your permission. **You may choose to exclude your name from CRA lists for unsolicited credit and insurance offers.** Creditors and insurers may use file information as the basis for sending you unsolicited offers of credit or insurance. Such offers must include a toll-free phone number for you to call if you want your name and address removed from future lists. If you call, you must be kept off the lists for two years. If you request, complete, and return the CRA form provided for this purpose, you must be taken off the lists indefinitely. **You may seek damages from violators.** If a CRA, a user or (in some cases) a provider of CRA data, violates the FCRA, you may sue them in state or federal court.

The FCRA gives several different federal agencies authority to enforce the FCRA:

FOR QUESTIONS OR CONCERNS REGARDING	PLEASE CONTACT
CRAs, creditors and others not listed below	Federal Trade Commission, Consumer Response Center- FCRA, Washington, DC 20580 * 202-326-3761
National banks, federal branches/agencies of foreign banks (word "National" or initials "N.A." appear in or after bank's name)	Office of the Comptroller of the Currency Compliance Management, Mail Stop 6-6 Washington, DC 20219 * 800-613-6743
Federal Reserve System member banks (except national banks, and federal branches/agencies of foreign banks)	Federal Reserve Board, Division of Consumer & Community Affairs Washington, DC 20551 * 202-452-3693
Savings associations and federally chartered savings banks (word "Federal" or initials "F.S.B." appear in federal institution's name)	Office of Thrift Supervision Consumer Programs, Washington D.C. 20552* 800- 842-6929
Federal credit unions (words "Federal Credit Union" appear in institution's name)	National Credit Union Administration 1775 Duke Street , Alexandria, VA 22314 * 703-518-6360
State-chartered banks that are not members of the Federal Reserve System	Federal Deposit Insurance Corporation Division of Compliance & Consumer Affairs Washington, DC 20429 * 800-934-FDIC
Air, surface, or rail common carriers regulated by former Civil Aeronautics Board or Interstate Commerce Commission	Department of Transportation Office of Financial Management Washington, DC 20590 * 202-366-1306
Activities subject to the Packers and Stockyards Act, 1921	Department of Agriculture Office of Deputy Administrator-GIPSA Washington, DC 20250 * 202-720-7051

Attachment 2

Table 1: Which Investigation to Request

If the requirement is for	And the person has this access	Based on this investigation	Then the investigation required is	Using standard
CONFIDENTIAL, SECRET, "L"	NONE	NONE	ANACI	A
	CONF, SECRET, "L"	Out of date ANACI or SSBI		
TOP SECRET, SCI, "Q"	NONE	NONE	SSBI	B
	NONE; CONF, SECRET, "L"	Current or out of date ANACI		
	TS, SCI, "Q"	Out of date SSBI	SSBI-PR	C

Table 2: Reinvestigation Requirements

If the requirement is for	And the age of the investigation is	Type required if there has been a break in service of _____	
		0-23 months	24 months or more
CONFIDENTIAL	0 to 14 years, 11 months	None (NOTE 1)	NACLC
	15 years or more	NACLC	
SECRET, "L"	0 to 9 years, 11 months	None (NOTE 1)	
	10 years or more	NACLC	
TOP SECRET, SCI, "Q"	0 to 4 years, 11 months	None (NOTE 1)	SSBI
	5 years or more	SSBI-PR	

NOTE 1: As a minimum, review an updated SF 86 and applicable records. A reinvestigation (NACLC or Special Background Investigation-Periodic Reinvestigation [SBI-PR]) is not required unless the review indicates the person may no longer satisfy the standards of EO 12968.

Attachment 3

Department of the Treasury
Tax Check/Tax Audit Waiver Form

PRIOR TO COMPLETING THIS FORM, REVIEW THE TERMS OF THIS AGREEMENT.

By providing the information herein and by signing this waiver, I voluntarily authorize the Internal Revenue Service (IRS) to release the return(s) and return information indicated below. The return(s) and return information will be used concerning my appointment or employment by the United States Government. This waiver is made pursuant to 26 U.S.C. 6103(c), which permits the release of return(s) and return information, which would otherwise be confidential, to my designee.

I request that the IRS release return(s) and return information to the following:

_____

Name of Agency and his/her authorized representatives

The information I am consenting to release is:

1. Have I failed to file a Federal income tax return for any of the last three years for which filing of a return might have been required? (If the filing date for the most recent required return has not yet lapsed on the date the IRS receives this waiver and IRS records do not indicate a return filing for the most recent required return, the "last three years" will mean the three years preceding the year for which returns are currently being filed and processed.)

2. Were any of the returns in item 1 filed more than 45 days after the due date for filing (determined with regard to any extension(s) of time for filing?)

3. Have I failed to pay any tax, penalty or interest liability during the current or last three calendar years within 45 days of the date of which the IRS gave notice of the amount due and request for payment?

4. Am I now or have I ever been under investigation by the IRS for possible criminal offenses?

5. Has any civil penalty for fraud been assessed against me during the current or last three calendar years?

If the information, which is to be released, includes a "Yes" answer to any of the above five questions, I authorize the IRS to release any information pertaining to that question.

TD F 15-03.10

Name: _____ SSN: _____

Home Phone: _____ Work Phone: _____

Current Address: _____

_____ _____

If married and filing a joint return:

Spouse Name: _____ Spouse SSN: _____

Name and address shown on returns for the last three years (if different from above).

Year	Name	Address

Date Signed
(Note: Waiver invalid unless dated by the taxpayer and received by the IRS within 120 days of this date.

Signature of taxpayer authorizing the disclosure of return information

NOTE: ANY ALTERATION OF THIS DOCUMENT MUST BE ACCOMPANIED BY THE TAXPAYER'S INITIALS AND DATE.

This form is in compliance with the Privacy Act of 1974. Our authorized right to ask for this information is 5 U.S.C. 301 and Executive Order 10450, which established the criteria for sensitive Government positions. The information you supply by signing this release of information form will be used principally to aid in the completion of an investigation to determine your suitability for employment in the Federal service or for other employment purposes. Such purposes include, but are not limited to, a security clearance, evaluation of qualification, suitability, loyalty to the United States, eligibility for access to government information, facilities, or information technology systems, or congressional inquiries. The information obtained may be re-disclosed to other Federal agencies for the above purposes and to the extent that is authorized by law.

Your signature on this release is voluntary, however, your failure to complete this form may mean that the required information cannot be obtained to complete your investigation. This may affect your placement or security clearance prospects.

TD F 15-03.10

Chapter II Section 2 **Investigative Requirements for Federal Employees, Contractors, Subcontractors, Experts, Consultants and Paid/Unpaid Interns** Updated 7/28/11

1. Introduction

The purpose of this section is to describe investigative requirements for Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns, who require staff-like access, wherever the location, to (1) Treasury/bureau-owned or controlled facilities; or (2) work on contracts that involve the design, operation, repair or maintenance of information systems; and/or (3) require access to sensitive but unclassified information.

Investigative requirements described herein also apply to personnel employed by United States boards/commissions/committees, regulatory corporations/boards/enterprises, federally funded research and development centers and federally chartered entities, for example: Smithsonian Institution, Federal Reserve, Legal Services Corporation, State Justice Institute, and United States Institute of Peace.

This section does not prescribe policy with respect to issuance of security clearances for access to classified National Security information under the National Industrial Security Program (NISP). See Chapter IV.

2. Scope

The provisions in this section apply to all bureaus, the Office of Inspector General (OIG), the Office of Treasury Inspector General for Tax Administration (TIGTA), and the Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) hereafter referred to as "bureaus." This section does not affect authorities reserved to the Assistant Secretary (Office of Intelligence and Analysis).

3. Requirements

a. The Contracting Officer's Technical Representative (COTR), in conjunction with the appropriate Departmental Offices (DO)/bureau management and the corresponding personnel security officer will review the work to be performed under contract and assign the highest risk designation to the entire contract in accordance with the criteria in Chapter I, Section 2, Position Sensitivity and Risk Designation. Each Federal employee, contractor, subcontractor, expert, consultant, and paid/unpaid intern will undergo investigative processing based on the works risk level designation.

b. The level to which such contractors, subcontractors, experts, consultants, and paid/unpaid interns are investigated shall be comparable to that required for Federal employees who occupy the same positions and who have the same position sensitivity designation. This includes contractors, subcontractors, experts, consultants, and paid/unpaid interns who have access to information or passwords associated with DO/bureau IT systems, designated sensitive positions, including off-worksite access.

c. All Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns are subject to a background investigation to determine their suitability and fitness for DO/bureau work and the investigation must be favorably adjudicated. Investigation of contractors, subcontractors, experts, consultants, and paid/unpaid interns will be conducted by employees of any of the following:

(1) The hiring DO/bureau.

(2) Another Federal agency.

(3) A contracting firm knowledgeable of the background investigations program that has been selected by the hiring DO/bureau, in consultation with the Office of Security Programs (OSP).

(4) An agency/company delegated by the individual DO/bureau Security Officer.

DO/bureau personnel security officers, in consultation with the COTR, Computer Security Officer, or appropriate DO/bureau official are to weigh potential risks and the magnitude of loss or harm that could be caused by individual Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns and determine risk levels for the DO/bureau facilities, information systems, and sensitive but unclassified information. Each DO/bureau has the final authority to designate the minimum requirements for their respective Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns background investigations.

d. DO/bureaus shall establish procedures to ensure information contained in the forms submitted by Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns for background investigations is treated in a confidential manner. It is the Department's policy that such information should only be available for review by employees of the DO/bureau security office.

e. Responsibility for adjudication of the background investigations shall remain with the DO/bureau personnel security officer or delegated authority. This applies to, but is not necessarily limited to end-product vendors but all Federal employees,

contractors, subcontractors, experts, consultants, and paid/unpaid interns. Individuals hired as Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns shall be subject to the same requirements as DO/bureau employees for the purpose of determining position sensitivity/risk and investigative requirements and shall not be processed through the NISP.

f. DO/bureaus shall establish and maintain a personnel security file for each individual Federal employee, contractor, subcontractor, expert, consultant, and paid/unpaid intern in (1) all national security positions; (2) all moderate and high risk public trust positions; and (3) those low risk or non-sensitive positions on whom unfavorable or derogatory information has been developed or received unless the file is maintained by the Office of Personnel Management (OPM). DO/bureaus need not maintain a file on a Federal employee, contractor, subcontractor, expert, consultant, and paid/unpaid intern granted access to classified information under the NISP, unless there is a requirement (1) for additional investigation in connection with access to DO/bureau facilities or IT systems; or (2) for access to classified information not covered under the NISP.

With regard to favorable investigations on Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns in low or moderate risk positions, DO/bureaus may, at their discretion, retain either the entire report or pertinent investigative data only. The specific location of personnel security files shall be at DO/bureau discretion with the following exception: all national security files shall be maintained by the DO/bureau security officer.

g. DO/bureau building service Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns whose duration of employment exceeds 30 days shall undergo, at a minimum, limited criminal history background checks as a condition for U.S. Government work. Such checks shall be based upon a technical search of the fingerprint files maintained by the FBI.

h. Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns who are screened for DO/bureau work shall ***not*** be considered to have been granted security clearance for access to classified information on the basis of the successful completion of any required investigation under this section.

i. Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns requiring access to DO/bureau facilities in foreign countries who have been certified by the Department of State Diplomatic Security Service as meeting investigative and adjudicative criteria for access to facilities under the authority of a Chief of Mission shall be deemed to meet personnel security standards.

4. Honoring Security Clearances

DO/bureau personnel security officers shall honor a Federal employee's, contractor's, subcontractor's, expert's, consultant's, and paid/unpaid intern's valid security clearance for access to classified information issued by other United States Government agencies or departments, provided the investigative basis for the clearance is current and meets investigative requirements. Additional investigation may be necessary if the investigation upon which the Federal employee's, contractor's, subcontractor's, expert's, consultant's, and paid/unpaid intern's security clearance was based is not sufficient for that needed for access to DO/bureau facilities, IT systems, and/or sensitive information.

5. Citizenship Requirements

a. Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns hired for work within the United States or its territories and possessions and who require access to DO/bureau-owned or controlled facilities, IT systems or security items or products, shall either be U.S. citizens or have lawful permanent resident alien status (green card holders).

b. DO/bureaus shall adhere to the following standard when allowing Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns access to DO/bureau-owned or -controlled facilities, IT systems, or security items or products.

(1) Low Risk = U.S. Citizen or lawful Permanent Resident Alien.

(2) Moderate Risk = U.S. Citizen or lawful Permanent Resident Alien with at least three or more years of U.S. residency from the date of legal entry to the U.S.

(3) High Risk = U.S. Citizen.

c. Only under exceptional circumstances should a waiver be requested when a Federal employee, contractor, subcontractor, expert, consultant, and paid/unpaid intern does not meet the citizenship or lawful permanent resident alien status requirement. Requests for waivers to the citizenship requirement must be submitted in writing. Foreign nationals employed as Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns shall not be allowed access to DO/bureau-owned or controlled facilities, IT systems, or security items or products prior to the issuance of a waiver.

d. Waivers for noncitizens performing in low-risk/non-sensitive positions may be requested in writing by COTRs through the DO/bureau security officer to the Director, OSP for determination.

e. Waivers for noncitizens performing in moderate-risk positions shall be requested in writing by the COTR, through a senior executive-level (SES) manager in the business unit that has the contract or through the DO/bureau head, to the Director, OSP for determination.

f. Waivers for access to high-risk positions will ***not*** be considered for foreign nationals.

g. Waivers for foreign nationals working in IT positions involving the development of DO/bureau hardware or software products will not be considered if the position involves the design of security models, application integration, customization of software or hardware, or configuration of servers or networks. Waivers will not be allowed if the position has the ability to manipulate, or alter or affect the integrity; accessibility or availability of IT maintained information or records.

h. All waivers involving IT systems must also be routed though Treasury's Chief Information Officer for review prior to approval by the Director, OSP and final determination.

i. All waiver requests must include the following:

(1) The full name, date of birth, place of birth, and current citizenship of the applicant.

(2) A completed SF 85, SF 85P, or SF 86.

(3) A completed background investigation.

(4) A description of the job/duty to be performed.

(5) Justification why there is no qualifying U.S. citizen or lawful permanent resident alien available or capable of performing the task.

(6) A business case necessitating the waiver.

(7) An assessment of the risk associated with granting the waiver.

(8) All security countermeasures and actions taken to mitigate the risks associated with the requested waiver.

6. Solicitations and Contracts

Solicitations and contracts shall include an appropriate caveat that contractor, subcontractor, expert, consultant, and paid/unpaid intern screening is required for access to DO/bureau facilities, IT systems, security items and products, and/or sensitive information. The caveat shall require the successful contractor, subcontractor, expert,

consultant, and paid/unpaid intern to execute appropriate security forms prescribed by the DO/bureau personnel security component (1) prior to work being performed; and (2) in advance of being granted access to DO/bureau facilities, IT systems, and/or sensitive information.

7. Adverse Information and Revocation of Access

a. When adverse information is developed in the course of an investigation, the scope of the inquiry will normally be expanded to the extent necessary to obtain such additional information as may be required to determine whether the Federal employee, contractor, subcontractor, expert, consultant, and paid/unpaid intern may be employed and granted access to DO/bureau facilities, IT systems, security items and products, and/or sensitive information.

b. A Federal employee, contractor, subcontractor, expert, consultant, and paid/unpaid intern on whom unfavorable or derogatory information has been developed during a personnel investigation must be so advised and offered an opportunity to refute, explain, clarify, or mitigate the information in question. The individual should also be advised that neither the nature of the information or the results of the interview, if he/she is denied employability on the U.S. Government-funded contract, will be conveyed by the DO/bureau to the employing company or any representative of the firm. However, if after final adjudication, a determination is made of ineligibility to render services and access to DO/bureau facilities is denied, the person will be formally notified and informed of the decision and the reason(s).

c. When denial of Federal employee staff-like access is appropriate, the contractor, subcontractor, expert, consultant, and paid/unpaid intern shall be informed, simultaneously with notification to the employing company that the individual is denied access for reasonable cause. The company shall be notified that the finding makes the individual ineligible to render services or otherwise perform work. The government may not disclose any details of the adverse information to the employing firm. This decision of the U.S. Government does not intend to imply that the contractor's, subcontractor's, expert's, consultant's, and paid/unpaid intern's suitability for employment elsewhere in the company is affected.

d. Access to DO/bureau facilities, IT systems, security items and products, and sensitive information is a privilege. It may be revoked by the affected DO/bureau based upon unsanctioned, negligent or willful action on the part of a Federal employee, contractor, subcontractor, expert, consultant, and paid/unpaid intern. Examples of actions that can trigger revocation include, but are not limited to, exploration of a sensitive system and/or data, introduction of unauthorized and/or malicious software, unauthorized modification or disclosure of IT systems and/or data, or failure to follow prescribed access control policies or procedures.

8. Nondisclosure Agreement for Sensitive Information

a. DO/bureau personnel security officers, in consultation with DO/bureau IT systems security officers, contracting officers, and COTRs, shall determine whether sensitive information to which Federal employees, contractors, subcontractors, experts, consultants, and paid/unpaid interns require access, warrants execution of a nondisclosure agreement as a condition thereof. When determined to be necessary following review and approval of DO/bureau legal counsel, each non-disclosure agreement will reference to the conditional nature of access to sensitive information with respect to the work, or specialized project, for which such access is required.

b. A sample nondisclosure agreement is shown in Attachment 1.

(1) DO/bureaus may draft and execute their own agreements; however, the use of a nondisclosure agreement other than Attachment 1 requires review and approval by appropriate DO/bureau legal counsel and the Director, OSP prior to use.

(2) If Attachment 1 is used the DO/bureau may only modify it by insertion of specific language in blank or parenthetical spaces relative to the contract, contracting DO/bureau or project. Other modifications require appropriate DO/bureau legal counsel and Director, OSP approval.

c. The original signed non-disclosure agreement shall be retained in the DO/bureau personnel security file for minimum of five years and for at least as long as the Federal employee, contractor, subcontractor, expert, consultant, and paid/unpaid intern has access to the facility, IT system or security items or products for which they executed the agreement. The DO/bureau has the discretion to maintain the agreement for as long as the information is deemed sensitive. A copy may be maintained in the official contract file. If requested, a copy may be furnished to the individual signatory.

d. DO/bureaus shall consult with legal counsel to determine whether annual appropriations acts, in effect at the time an agreement is executed, contain provisions requiring the inclusion of specific text in nondisclosure agreements.

Attachment 1

(Project or Contract Name/Number)
Conditional Access to Sensitive Information
Non-disclosure Agreement

I, _____, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain United States Government documents or material containing sensitive information.

I understand and agree to the following terms and conditions:

1. By being granted conditional access to sensitive information, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement.

2. As used in the Agreement, sensitive information is any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. 522a, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

3. I am being granted conditional access contingent upon my execution of this Agreement for the sole purpose of (identify the nature of contract work or special project). This approval will permit me conditional access to certain information, (identify type(s) of information, e.g., documents, memoranda, reports, testimony, deliberations, maps, drawings, schematics, plans, assessments, etc.) and/or to attend meetings in which such information is discussed or otherwise made available to me.

4. I will never divulge any sensitive information that is provided to me pursuant to this Agreement to anyone unless I have been advised in writing by (identify the bureau or in the case of bureau sensitive information released to the Office of Inspector General (OIG) or Treasury Inspector General for Tax Administration (TIGTA), or the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) in accordance with a written arrangement related to the official audit/investigative functions of the OIG or TIGTA or SIGTARP for that particular matter). Should I desire to make use of any sensitive information, I will do so in accordance with paragraph 6 of this Agreement. I will submit to the (identify DO/bureau) for security review, prior to any submissions for publication, any book, article, column or other written work for general publication that is based upon any knowledge I obtained during the course of my work on (name the project) to ensure that no (identify DO/bureau) sensitive information is disclosed.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of sensitive information not consistent with the terms of this Agreement.

6. Upon signing this non-disclosure agreement, I will be permitted access to official (identify DO/bureau) documents containing sensitive information and understand that any copies must be protected in the same manner as the originals. Any notes taken during the course of such access must also be protected in the same manner as the originals.

7. If I violate the terms and conditions of this Agreement, I understand that the unauthorized disclosure of sensitive information could compromise (identify DO/bureau) security.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to sensitive information. This may serve as a basis for my being denied conditional access to the (identify DO/bureau information, both classified and sensitive information in the future. If I violate the terms and conditions of this Agreement, the United States may institute a civil action for damages or any other appropriate relief. The willful disclosure of information to which I have agreed herein not to divulge may constitute a criminal offence.

9. Unless and until I am provided a written release by the (identify DO/bureau) from this Agreement or any portions of it, all conditions and obligations contained in this Agreement apply both during my period of conditional access, which shall terminate at the conclusion of my work on (name of project/contract), and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provisions of this Agreement unenforceable, all other provisions shall remain in full force and effect.

11. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

12. By granting me conditional access to information in this context, the United States Government does not waive any statutory or common law evidentiary privileges or protections that it may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

13. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 13526 or 13556; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.)(governing disclosures that could expose confidential Government agents), and the statutes that protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 128, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50

USC Section 783 (b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. My execution of this Agreement shall not nullify or effect in any manner any other secrecy or nondisclosure Agreement which I have executed or may execute with the United States Government except within the Department of the Treasury as noted in item 8, above.

15. I make this Agreement in good faith, without mental reservation or purpose of evasion.

Name _____ Date _____

Signature _____

This Agreement was accepted by the undersigned on behalf of the (Treasury Department or identify bureau) as a prior condition on conditional access to sensitive information. Further release to any other third party requires execution of a nondisclosure agreement.

When information is shared with the Office of Inspector General or the Treasury Inspector General for Tax Administration or the Special Inspector General for TARP, for official audit/investigative purposes, the following statement must be added below the signature line. "This Agreement was accepted by the undersigned on behalf of the (identify bureau and (the Office of Inspector General or Treasury Inspector General for Tax Administration, Special Inspector General for TARP, as applicable) for conditional access to sensitive information. Further release and dissemination of (identify DO/bureau) sensitive information under this non-disclosure agreement must be in accordance with a written arrangement related to the official audit/investigative functions of the OIG or TIGTA or SIGTARP for that particular matter. Further release to any other third party requires execution of a nondisclosure agreement."

(IdentifyDO/bureau signatory _____ Date _____

(OIG or TIGTA or SIGTARP signatory) _____ Date _____

Security Manual

Chapter II
Section 3

Personnel Security Investigative Policy for Treasury Communications Contractor and Subcontractor Personnel

TD P 15-71

1. Introduction

The purpose of this section is to establish the personnel security and investigative requirements for contractor and subcontractor personnel who require access to designated Treasury/bureau, other Government agencies, or commercial locations in connection with the design, development, implementation, maintenance, or management of the Treasury Communications System (TCS), the successor to the Consolidated Data Network (CDN). The intent is to eliminate the need for Treasury/bureaus to conduct duplicate investigations for TCS contractor personnel.

2. Requirements

a. The Internal Revenue Service (IRS) has the primary responsibility for conducting background investigations of TCS contractor employees.

b. The Assistant Director (Personnel Security), Office of Security Programs (OSP), has final responsibility for adjudication and certification of individuals to the TCS Prime Contractor.

c. The prime contractor will assume the primary responsibility for certifying contractor accesses to TCS user agencies in accordance with paragraph 8 of this section.

d. Treasury/bureau TCS user agency/organizations shall be responsible for providing necessary escort(s) as required for particular contractor personnel.

3. Risk Assessment

Different types of background investigations, varying in scope, have been identified and are required for positions based on the associated risk level. Risk is assessed according to the degree of access to information and facilities, as follows:

a. *Low-Risk.* This level includes personnel who require access to TCS facilities only to perform support functions, such as facility cleaning or maintenance, mail service, or warehouse service. Such personnel do not require and shall not be provided access to TCS information, the TCS Network, or the internal Local Area Network (LAN).

b. *Moderate-Risk.* This level includes all personnel who require access to TCS information or access to the TCS LAN within the TCS Communications Center (TCC), but do not require access to the Network Control Center (NCC) or to the TCC Security Facility (TSF). This also includes contractor personnel who require access to User facilities, but not to communications security (COMSEC) keying material.

c. *High-Risk.* This level includes all personnel who require access to COMSEC keying material, access to the NCC or the TSF, or access in any similar capacity to any associated TCS backup or development facility. Also included are persons who are performing security functions or program management roles, or are responsible for directing or managing development, maintenance, or operation of TCS systems.

Results of sample risk assessments associated with position and type of access within TCS are identified in Attachment 1, *Sample TCS Position Risk Matrix.*

Background investigation and re-investigation requirements associated with the various risk levels are described in paragraph 5. Paragraph 6 describes provisions for acceptance of previous investigations and interim access approval.

4. Adjudication Criteria

a. Except as described in paragraph 5b, below, investigations will be adjudicated by the Assistant Director (Personnel Security), OSP according to criteria set forth in Title 32 Code of Federal Regulations Part 147, Subpart A, *Adjudicative Guidelines.* See Chapter I, Section 3.

b. The TCS contract requires that all contractor and subcontractor personnel (1) working on TCS development, implementation, and maintenance; and/or (2) having unescorted access to contractor-operated TCS facilities, must be United States citizens.

5. TCS Background Investigations Requirements and Descriptions

There are five types of background investigations selected for contractor personnel supporting the program. Submitted forms shall be the same for all levels of investigation. A brief description of the scope of each investigation follows.

a. *Basic Investigation.* This investigation serves as the full investigation for personnel in Low-Risk support positions not requiring access to the network or TCS information. Also, it provides the basis for interim access approval for those personnel awaiting completion of a Minimum Background Investigation (MBI) or Background Investigation (BI), as described in paragraph 7. The investigation is used in the conversion process described below. The scope of this investigation

shall be as follows:

(1) Review of SF 85P/SF 85P-S.

(2) Criminal History Check (fingerprint card for the Federal Bureau of Investigation [FBI]).

(3) NCIC (Interstate Identification Index and Wanted Persons File).

(4) OPM Security Investigations Index (SII) Search.

(5) Defense Clearance and Investigations Index (DCII) Search.

(6) IRS Integrated Data Retrieval System (IDRS) Search.

(7) Credit Check.

b. *Minimum Background Investigation (MBI).* This investigation shall be required for personnel in Moderate-Risk positions not requiring NCC access. The scope of this investigation shall be as follows:

(1) All elements of the Basic Investigation.

(2) Local Agency Check (five years by voucher).

(3) Employment Verification for past five years (by voucher)

(4) Education, highest attended verified (by voucher).

(5) Listed references, minimum two, (by voucher).

c. *Background Investigation (BI).* This investigation shall be required for personnel in High-Risk positions requiring access to the NCC, the TSF, and/or COMSEC keying material. The scope of this investigation shall be as follows:

(1) All elements of the Basic Investigation.

(2) Local Agency Check (five years by voucher).

(3) Employment verification for past five years.

(4) Education verification, highest attended.

(5) References, minimum four; two listed and two developed.

(6) Neighborhood checks.

d. *TCS Reinvestigations*. All TCS contractor personnel will undergo a reinvestigation five years after the completion of their most recent TCS investigation. The scope of this investigation will be identical for all levels of access and to the Basic Investigation, plus Local Agency Checks (five years by voucher).

e. *Additional Checks*. Treasury/bureaus may perform such additional checks as may be necessary for access to certain user facilities. However, any such additional screening criteria and processes, or for modification of these personnel security policies, shall be made only with the approval of the Director, OSP.

6. Acceptance of Previous Investigations

Previous background investigations conducted by other U.S. Government agencies, of the same or greater scope as the required TCS background investigation, will be accepted as satisfying investigative requirements for any TCS position. Treasury/bureaus must complete a "Checklist of Permitted Exceptions to Reciprocity". See Chapter 1, Section 4 prior to requesting additional information, security forms, or investigations on individuals with prior background investigations

7. Interim Access Approval

Interim access approval will be certified to the TCS Prime Contractor by the Assistant Director (Personnel Security), OSP prior to completion of the full investigation. The only authorized positions for interim approval are given in Attachment 1.

Interim access approval is granted as follows:

a. Individuals who posses a current U.S. Government security clearance for access to classified information at the *Top Secret* level may be granted interim approval to occupy positions designated High-Risk, as specified in Attachment 1, upon favorable review of the current SF 85P and verification of the security clearance by the Assistant Director (Personnel Security), OSP.

b. Individuals who possess a current U.S. Government security clearance for access to classified information at the *Confidential* or *Secret level* may be granted interim approval to occupy positions designated Low-Risk or Moderate-Risk, respectively, upon favorable review of the current SF 85P and verification of the security clearance by the Assistant Director (Personnel Security), OSP.

c. Individuals not possessing a current U.S. Government security clearance for access to classified information may be granted interim approval to occupy positions designated Low-, Moderate-, or High-Risk, as specified in Attachment 1, upon favorable completion of the Basic Investigation.

8. Visit Certifications

The TCS contract requires the prime contractor to dispatch contractor personnel to Treasury/bureau sites and facilities to perform installation, maintenance, and other related activities for the TCS program. Authorized access to Treasury/bureau sites and facilities shall be coordinated and certified in the following manner:

a. Treasury/bureaus shall identify a security office or other point-of-contact (POC) for the TCS program responsible for receiving and maintaining TCS visit authorizations certified by the TCS prime contractor's security office. Large and/or regionally dispersed Treasury/bureaus may need to identify multiple security POCs.

b. The TCS prime contractor's security office will (1) certify contractor TCS accesses to each responsible Treasury/bureau security office; and (2) provide timely notification of access terminations to the responsible Treasury/bureau security office. Access authorizations passed to Treasury/bureau security offices are verifiable through the Assistant Director (Personnel Security), OSP.

c. Specific TCS service request activities will be coordinated with each site POC by the TCS prime contractor organization which will provide to the site POC the identity of the contractor employee and the requested dates and/or times of site access.

Attachment 1

Sample TCS Position Risk Matrix

This matrix identifies typical levels of risk associated with information and system/network accesses within the TCS program.

Facility Access (1)				*Position Description*	*Level of Risk*	*BI Type*	*Interim Approval (2)*
TSF	*NCC*	*EBF*	*TCC*				
X	X	X	X	System and Security Administrator	High	BI	No
X	X	X	X	COMSEC Management Operations	High	BI	No
X	X	X	X	Security S/W or H/W Development	High	BI	No
X	X	X	X	Shift Supervisors	High	BI	No
X	X	X	X	Security Operator	High	BI	No
X	X	X	X	Operations Management	High	BI	Yes (3)
X	X	X	X	Program Management	High	BI	Yes (3)
X	X		X	Building Guard Force (5)	High	BI	Yes
	X	X	X	Network Monitor/Control Personnel	High	BI	Yes
	X	X	X	Database Administrator (DBA)	High	BI	Yes
	X	X	X	General S/W Development	High	BI	Yes
	X	X	X	H/W Development	High	BI	Yes
	X	X	X	Test Engineer I	High	BI	Yes
	X	X	X	Design Engineer I	High	BI	Yes
	X	X	X	Help Desk Personnel I	High	BI	Yes
	X	X	X	Customer Service I	High	BI	Yes
	X	X	X	Service Request I	High	BI	Yes
				Field Engineers, COMSEC	High	BI	Yes (4)
			X	Test Engineer II	Moderate	MBI	Yes
			X	Design Engineer II	Moderate	MBI	Yes
			X	Help Desk Personnel II	Moderate	MBI	Yes
			X	Customer Service II	Moderate	MBI	Yes
			X	Service Request II	Moderate	MBI	Yes
				Field Engineers, General	Moderate	MBI	Yes (4) 5?
			X	Program Administrator	Moderate	MBI	Yes
			X	Billing Services	Moderate	MBI	Yes
			X	Mail Services	Low	Basic	N/A
			X	Warehouse Services	Low	Basic	N/A/
			X	Facility Maintenance/Housecleaning	Low	Basic	N/A

Notes:

(1)	TSF TCC Security Facility, network access NCC Network Control Center, network access EBF Emergency Backup Facility, network access TCC Building access, facility LAN, no network access
(2)	Interim access approval is based on successful completion of the Basic Investigation.
(3)	Interim access approval is for NCC only; TSF access requires completed BI.
(4)	Field Engineers will not normally require access to contractor operated TCS facilities. Access will be to Government facilities.
(5)	Access to NCC/TSF in emergencies only.

Chapter III Section 1 — **Prerequisites for Accessing and Processing Classified Information** — Updated 6/17/11

1. Introduction

Under Executive Order (EO) 13526, Classified National Security Information, dated December 29, 2009 or prior Orders, classified information shall be afforded a level of protection against unauthorized access and disclosure commensurate with its level of classification. Except as consigned to temporary Federal records storage or until fully accessioned into the National Archives of the United States, Departmental Offices (DO)/bureau-originated classified information remains the responsibility of and is controlled by the originating DO/bureau component.

2. Eligibility for Access

EO 12968, Access to Classified Information, dated August 2, 1995 provides that to be eligible for access to classified information distinct actions must be taken. EO 13526 further reiterates that individuals must have:

- A favorable determination of eligibility for access.
- Signed Standard Form (SF) 312, *Classified Information Non-Disclosure Agreement.*
- The need-to-know the information.
- Participated in contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized access. Additionally, employees who are Original Classification Authorities (or OCAs) must receive proper classification and declassification training at least once annually.

A security clearance for access to classified information shall not be fully valid until each of the four elements is fulfilled. Each of the required elements is discussed in more detail below.

3. Determination of Need-to-Know

Need-to-know is a determination within the Executive Branch in accordance with directives issued pursuant to EOs 12968 and 13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized U.S. Government function.

4. Determination of Trustworthiness

An individual is eligible for access to classified information only after a positive showing of trustworthiness as determined by proper DO/bureau authority and based upon an investigation (and favorable adjudication) in accordance with National personnel security standards, criteria and accompanying Treasury guidance.

5. Classified Information Non-disclosure Agreement (SF312)

Completion of the SF 312 is required before the U.S. Government may grant an individual access to classified information. DO/bureaus shall retain executed copies of the SF 312 in file systems from which the agreement can be expeditiously retrieved in the event the U.S. Government must seek its enforcement because of a breach of the agreement.

Copies or legally enforceable facsimiles of the SF 312 shall be retained for 50 years following the date of signature. The requirements of the SF 312 are a lifetime commitment – they do not expire or lapse with the signer's departure from or termination from U.S. Government employment or service.

6. Contemporaneous and Refresher Security Training

Individuals meeting the requirements in paragraph 2 above must receive contemporaneous training on the proper safeguards to protect classified information, i.e., handling, processing, marking, storing, accounting/tracking, and destruction, etc. Additionally, individuals shall participate in periodically assigned refresher training as mandated by the Director, Office of Security Programs and/or bureau security officials.

7. Termination of Security Clearance

Access to classified information shall be terminated when an individual no longer has the need-for-access. Departing individuals shall receive a termination briefing to impress upon them the continuing responsibility not to disclose any classified information to which the employee or contractor personnel had access, the potential penalties for non-compliance; and the obligation to return all classified documentary material (including that originated and/or derived by, and/or physically provided to them) in the individual's possession to appropriate officials. Upon completion of the debriefing, the employee shall sign the security debriefing acknowledgment portion of SF 312. Departing employees shall also turn over the combination to any security equipment storing classified information to their supervisor to avoid possible lock-outs and costly repairs.

8. DO/bureau Processing of Classified Information

Classified information may ONLY be processed on approved computers/equipment, i.e., the Treasury Secure Data Network (TSDN) for Secret and Confidential information (as well as particularly sensitive information) or the Treasury Foreign Intelligence Network (TFIN) for Top Secret and Sensitive Compartmented Information.

9. Treasury Directive Publications 85-01, Volume and 15-03

For information on uniform procedures to ensure automated information systems, including networks and telecommunications systems that collect, create, communicate, compute, disseminate, process, or store classified information, prevent unauthorized access, ensure information integrity, and to the maximum extent practicable, use common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the formats to maximize the accessibility of information to persons who meet the standards set by EO 13526 for access to classified information, please refer to TD P 85-01, Volume II and TD 15-03 and/or contact the DO, Office of the Chief Information Officer (OCIO).

Chapter III **Mandatory Security Awareness Training** Updated
Section 2 5/15/14

1. Introduction

Executive Order (EO) 13526 mandates the establishment and maintenance of security education and training for persons authorized access to classified information. All Departmental Offices (DO)/bureau employees must receive security awareness training commensurate with their duties and the classification or sensitivity of the information, assets, and/or facilities to which they have access. An employee's success in protecting classified and sensitive information and resources depends largely on their understanding of (1) what needs protecting; (2) why, (3) who to protect it from; and, (4) how they must protect it.

Further, the performance contract used to rate employees requires the designation and management of classified information as a critical element or item to be evaluated in rating original classification authorities, security managers or security specialists, and all other personnel whose duties significantly involve creation or handling of classified information; including personnel who regularly apply derivative classification markings in the drafting, deliberative process, review and finalization.

2. Responsibility for Security Awareness Training

DO/bureaus are responsible for ensuring the following tasks are carried out with regard to security awareness training:

- Developing and implementing security awareness training provided by the Director, Office of Security Programs and modifying same, (including funding) as appropriate, for incorporation within their bureau security awareness and training.
- Designating primary and alternate persons responsible for maintaining their security awareness training programs.
- Creating/retaining records documenting all employee/contractor personnel security awareness training they provide/sponsor.
- Establishing sufficient controls to ensure supervisors/managers are held accountable for their employees receiving appropriate security awareness training.
- Periodically analyzing the effectiveness of their security training programs.
- Annually reporting on security awareness training programs as may be requested by the Director, OSP.

The types of training programs (their content and required audiences) include, but are not necessarily limited to, those described in paragraphs 5 through 11 of this section. Training modules have been developed by OSP for a variety of audiences and along with several guidance documents/directives are posted on the OSP website under "education and training" at http://thegreen.treas.gov/programs/Pages/training.aspx and listed under "publications, references and resources" at http://thegreen.treas.gov/programs/Pages/publications.aspx DO/bureaus are free to use and/or adapt these modules to fit end-user's unique office working conditions.

NOTE: The Director, Special Security Programs (SSP) within the Office of Intelligence and Analysis (OIA) is responsible to ensure SCI refresher training is conducted annually for all DO/bureau SCI indoctrinated personnel.

3. Training Records and Analyses

Records shall be established and maintained for all types of security awareness training covering the life-cycle of an employee's tenure with DO/bureaus, preferably in a centralized database that is maintained by the DO/bureau security component. The records shall enable adequate analyses of the effectiveness of information given in particular training, methods used, and quick (one-stop) reconstruction of an employee's specific training history for the duration of DO/bureau employment. Training iterations shall be retrievable by employee name and covered in a corresponding system of records notice.

DO/bureau offices shall monitor the effectiveness of security training programs and be measured in terms of comparison/contrast with security incidents, infractions, violations, spills, and available feedback or commentary from employees. The effectiveness of security training shall also be included in self-assessments. DO/bureaus may also use opinion surveys and periodic computer-based training testing to evaluate employees' security knowledge and awareness.

NOTE: The Special Security Office (SSO) within SSP schedules SCI refresher training for all DO/bureau SCI indoctrinated personnel. The SSO also maintains records of attendance and monitors training effectiveness.

4. Audiences for Security Awareness Training

The audiences for security awareness training include the following people:

- Full and part-time DO/bureau employees.
- Consultants and contractor personnel accessing classified/sensitive information.
- Interns.

- Other U.S. Government agency employees on detail to DO/bureaus.
- Persons employed by State, local, tribal and private sector entities, and public sector representatives supporting a task force or other mandated group or activity within DO/bureaus.

Security awareness training for contractor personnel shall be in accordance with this section, and the training shall be related to the particular requirements of individual contracts involving access to classified/sensitive information. This also applies to program-specific training for: (1) consultants; (2) interns; (3) detailees and (4) representatives of State, local, tribal, private sector entities and public-supported task forces; and/or (5) other groups.

NOTE: All DO/bureau SCI indoctrinated personnel are required to attend annual SCI refresher training conducted by the SSP.

5. Initial Security Orientation

a. *Audience.* All DO/bureau employees shall receive initial orientation to security practices, procedures, and responsibilities within DO/bureaus prior to functionally reporting to the workplace. This training is regardless of the position occupied or the sensitivity of information and access to classified information that they might later have.

b. *Content.* Training shall be focused on new-hires to provide basic introduction to security, types of information they would need to report and to whom; building or facility access controls, and identification media. Training shall cover the new-hires' roles and to enable them to differentiate between classified and sensitive information they might possibly be inadvertently exposed to or overhear. Training shall concentrate, where appropriate, on sensitive information, including use controls, identification and markings, storage, general guidance for handling and processing sensitive information, disclosure, closing-hour checks, and destruction for all employees.

c. *Timeframes.* During new-hire orientation and periodically at discretion of the Director, Office of Security Programs or bureau security officials.

NOTE: Initial SCI indoctrination briefings are given to all DO/bureau new hire personnel who require access to SCI material to perform their duties. The briefings provide complete introductions to common IC security principles.

6. Contemporaneous Training for Access to Classified Information

a. *Audience.* All DO/bureau employees authorized access to classified information shall receive contemporaneous training on attendant security responsibilities for safeguarding classified information at the time they receive a security clearance.

b. *Content.* Training includes markings to properly identify classified information, handling, processing, storing, copying, accountability, receipting, transmitting, packaging, and destroying classified information. Training shall concentrate on using only approved information systems/equipment for classified processing (the Treasury Secure Data Network or the Treasury Foreign Intelligence Network), proximity controls, in-use controls, storage, dissemination/discussion, closing-hour checks, preventing security violations/spills, and destruction of classified information along with the civil, criminal, disciplinary, and administration actions that might result from non-compliance with DO/bureau security requirements. Training shall also reference the life-long commitment to protect classified information that an employee has had access to during their entire tenure and be included in any termination briefing they receive due to their departure, transfer, retirement, etc.

c. *Timeframes.* Training is required upon issuance of the employee's security clearance for access to classified information. Where the training is for an "interim" clearance, the employee does not need to attend the same training when their "final" clearance is issued. Refresher training is required every year or as otherwise mandated by the Director, OSP or bureau security officials.

NOTE: In conjunction with the initial SCI indoctrination briefing, a thorough briefing on local SCI-related security procedures and best practices is given by SSP security officials.

7. Annual Refresher/Periodic Training

a. *Refresher audience.* DO/bureau employees shall receive annual refresher training to remind them of security requirements for safeguarding classified information (including, as appropriate, on reporting/preventing spills).

b. *Refresher content.* Refresher training shall be DO/bureau-specific and focus on keeping employees current on established security policies and relevant events, as they relate to information, facilities, and assets to which they have access.

Refresher training may be provided in various formats, e.g., instructor-lead "talking head" presentations, CD-ROM or computer-based, global message reminders, and job aids such as pamphlets, posters, hand-outs, tent cards, and desk references suitable to the organization. Types of training may vary from year-to-year based on operational needs and the importance of particular security messages conveyed. Protective requirements for sensitive information shall also be included as appropriate to given audiences.

c. *Timeframes.* Periodic update training shall occur in conjunction with employee reinvestigations for access to classified information (every five years for holders of Top Secret clearance; every ten years for holders of Secret or Confidential clearance). Updates shall be directed at trends in violations or other non-

compliance with security policies. Refresher training may also be required by the Director, OSP or bureau security officials for those employees determined to have been responsible for a security violation.

NOTE: As part of a continuing security awareness, training and education program, annual SCI refresher training is given by the SSP to all DO/bureau SCI indoctrinated personnel.

8. Mandatory Training for Original Classifiers

a. *Audience*. All employees identified by position title in Treasury Order (TO) 105-19, *Delegation of Original Classification Authority; Requirements for Declassification and Downgrading* and DO/bureau officials annually designated as an Original Classification Authority (OCA) on Treasury Department Form (TD F) 15-05.2, *Report of Authorized Classifiers*.

OCAs who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended until such training has taken place. The Secretary, Deputy Secretary or Senior Agency Official (as identified in TO 105-19) may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented and when granted, the individual shall receive the required training as soon as practicable.

b. *Content*. Detailed training on proper classification and declassification, with emphasis on avoiding over-classification. At a minimum, the training shall cover classification standards, levels of classification, classification authority, categories, duration (setting a declassification date/event), identification and required markings (including identifying or describing damage), prohibitions and limitations, sanctions, classification challenges, developing (and updating) classification guides, handling, processing, accountability, safeguarding, reproduction, destruction, preventing security violations, use of attendant security forms and information sharing.

c. *Timeframes*. OCA training must be taken at least once each calendar year.

9. Required Training on Derivative Classification and Using Classification Guides

a. *Audience*. All DO/bureau employees who apply derivative classification markings; classification management officials, security managers, security specialists, declassification authorities (including applicable FOIA/PA personnel) and all other personnel whose duties significantly involve the creation or handling of classified information.

Derivative classifiers who do not receive such mandatory training at least once two years shall have their authority to apply derivative classification markings suspended until such training has taken place. The Secretary, Deputy Secretary or Senior Agency Official (as identified in TO 105-19) may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented and when granted, the individual shall receive the required training as soon as practicable.

b. *Content.* Training shall cover the proper application of derivative classification principles, emphasizing the avoidance of over-classification. At a minimum, the training shall cover the principles of derivative classification, identification and required markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, handling, processing, accountability, safeguarding, reproduction, transmission, destruction, preventing security violations, attendant security forms and information sharing.

c. *Timeframes.* Training shall be taken on derivative classification at least once every two years.

10. Termination Briefing

a. *Audience.* All departing, transferring, or retiring DO/bureau employees authorized access to classified information. Reasonable actions shall be taken to reach such employees prior to termination, including contacting the gaining organization for those transferring out of the Department.

b. *Content.* Training shall ensure employees are informed of their continued responsibilities to protect classified information that they had access to during their entire DO/bureau tenure. For those employees who might not be available at the time of their departure/transfer or retirement, the termination briefing shall be posted on DO/bureau security websites to receive wide dissemination and availability. Records in DO/bureau security files shall annotate the circumstances of any failure to provide the required termination briefing.

c. *Timeframe.* Training should be taken before employees' departure, transfer or retirement from employment with DO/bureau.

NOTE: When an individual no longer requires access to SCI material, the Debrief section of the Form 4414 will be signed and security debriefing will be conducted by the SSP.

11. Specialized Security Training

DO/bureau employees shall receive specialized security training within six months after assumption of duties warranting such training in the following areas:

- Practices applicable to official foreign travel.
- Counterintelligence training.
- Methods for dealing with un-cleared personnel who work in proximity to classified information (including hosting classified meetings).
- Responsibilities of employees serving as couriers of classified information.
- Responsibilities of DO/bureau employees issued (and in using) official credentials.
- Procedural requirements for safeguarding classified information processed and stored on approved DO/bureau information systems/equipment.
- Other security training, as mandated by the Director, OSP or bureau security officials.

Chapter III **Information Security Program Forms** Updated
Section 3 10/21/11

1. Introduction

This section identifies standard security forms and their prescribed use in protecting classified and sensitive information. This includes U.S. Government-wide Standard Forms (SFs) and required Treasury Department Forms (TD Fs). These forms apply to information the Departmental Offices (DO)/bureaus that is stored in security containers, on electronic/magnetic media, and hard-copy paper documents; or in fulfilling requirements when handling classified information in the course of official business.

2. Standard Form 311 – Agency Security Classification Management Program Data

The SF 311, *Agency Security Classification Management Program Data*, is a data collection form every Executive Branch agency annually submits to the Information Security Oversight Office, National Archives and Records Administration, to record the number of original classification authorities; original/derivative classification decisions; mandatory review requests; automatic, systematic and discretionary declassification reviews; internal oversight; classification guides and explanatory comments.

3. Standard Form 312 – Classified Information Non-disclosure Agreement

The SF 312, Classified Information Non-disclosure Agreement, is a binding agreement between the U.S. Government and all persons authorized access to classified information. As used in the Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526 or under any prior Executive order or statute that prohibits the unauthorized disclosure of information in the interest of the national security; and unclassified information that meets the standards for classification and is in the process of such a determination, or under any other Executive order or statute that requires protection for such information in the interest of national security.

NOTE: Personnel authorized access to SCI material will sign a Form 4414, Sensitive Compartmented Information Nondisclosure Agreement. This form, available from the Office of Special Security Programs, is signed at the initial SCI indoctrination as agreement to the terms outlined thereon. It is also signed at the individuals' debriefing when access to SCI material is no longer required.

4. Standard Form 700 – Security Container Information

The SF 700, *Security Container Information*, records vital information about the security container in which it is located. The form has three parts.

- Part 1 shall be completed in its entirety to reflect the name, address, and telephone number of DO/bureau employees responsible for classified contents. This part of the form shall be posted on the (inside) front of the control drawer of the General Services Administration (GSA)-approved security container or the (inside) front top drawer of any non-GSA-approved equipment.

- Part 2 is a protective envelope to store the combination.

- Part 2A shall record the actual combination of the container.

Both parts 2 and 2A shall have the appropriate level of classification (Top Secret, Secret, Confidential) stamped or affixed on them. On Part 2A the marking should appear above the word "WARNING"; on Part 2 it should appear in the top and bottom margins. Part 2A shall be placed in the envelope and hand-carried or sent via other secure means to the appropriate DO/bureau security officer responsible for centralized storage. DO/bureau security officials shall conduct periodic reviews to ensure records of security combinations on file are true and accurate. Supervisors are responsible for ensuring DO/bureau security officials are notified when departing employees leave or retire so that combinations are not lost or forgotten with such departures.

a. *Protecting Sensitive Information.* The SF 700 shall also be used to record information (including combinations) to equipment that protects sensitive information. In such instances the authorized sensitivity designation shall be annotated above the "WARNING" line and also in the top/bottom margins to differentiate the combination from security equipment storing classified information.

b. *Lock Combinations.* Combinations to equipment storing classified and other information protected by mechanical and electronic locks must be recorded on the SF 700. This is to ensure an official record is maintained to facilitate access to such equipment, prevent possible lockouts, and diminish the need to drill into (and effect costly repair) the lock/equipment when the combination is unknown, forgotten, and/or otherwise unavailable.

c. *Classifying Combinations.* Dial-type lock combinations shall be administratively classified at the highest level of classified information that is protected by the lock. The act of classifying the combination shall NOT be included in statistically reporting the volume of classified documents generated annually on Standard Form 311. Combinations shall be changed only by persons authorized access to the level of information protected unless other sufficient controls exist to prevent their further access to the lock and/or knowledge of the combination.

Combinations on in-service equipment shall be changed whenever any of the following occur:

- The equipment is placed into use.
- A person knowing the combination no longer requires access to it and other controls do not exist to prevent their access to the lock.
- The combination has been subject to possible unauthorized disclosure.
- When taken out of service, combination locks shall be reset to the standard combination 50-25-50 or 10-20-30 and the equipment inspected to ensure all classified and/or sensitive information remains inside.

5. Standard Form 701 – Activity Security Checklist

The SF 701, *Activity Security Checklist*, is a systematic means to thoroughly inspect a particular office or secure work area and to allow for DO/bureau employee accountability if any irregularities are discovered.

a. *Information included on SF 701.* The SF 701 includes space to indicate whether the following activities have been completed:

- Security containers have been locked or checked by authorized persons.
- Desks, wastebaskets, and other surfaces and receptacles are free of classified information.
- Windows/doors have been locked.
- Electronic media (such as disks, tapes, removable hard drives, etc.) for processing classified information have been properly stored.
- Security alarms and protective equipment are activated.

DO/bureaus may include additional information on the SF 701 to suit their unique circumstances.

b. Each security-approved "Open Storage" area safeguarding classified information and Sensitive Compartmented Information Facility (SCIF) shall use the SF 701 unless the area or facility is in continuous operation (24 hours a day, seven days a week). As with the SF 702, retention of completed SF 701s shall be determined by DO/bureau security officials. Within a SCIF, retention of the SF 702 is at the discretion of the Special Security Office (SSO) in Treasury's Office of Intelligence and Analysis (OIA).

6. Standard Form 702 – Security Container Check Sheet

The SF 702, *Security Container Check Sheet*, is a tool used in determining the identity of authorized DO/bureau persons responsible for safeguarding classified information and particularly the last person acknowledging having locked and secured the security equipment. The form provides a record of the identity and *actual time* authorized persons have opened, closed, and checked a particular security container authorized for storing classified information.

a. *Location of Check Sheet.* SF 702, *Security Container Check Sheet,* shall be conspicuously affixed to the outside of every security container or vault storing classified information. Except for the SF 702, the top surface area of all security equipment shall remain free of extraneous material to enhance the efficiency of closing-hour security checks.

b. *Recording Data on Check Sheet.* When an authorized person first opens the container on a given day, he or she shall record the date, the *actual time*, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the *actual time* and their own initials. Users shall avoid citations reflecting standard opening, locking and checking of the security equipment at routine times, e.g., opened at 9:00 AM and closed/checked at 5:30 PM.

   The use of all three columns of the SF 702 is encouraged, however, the "opened by" and "closed by" columns must be completed. Use of the "checked by" column is up to individual DO/bureau security offices to determine.

c. *Assessing Security.* On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment. Such examination might consist of a quick and casual visual check to note any obvious marks, streaks, gashes, or defects on the security container and its operation. Any discrepancies in the appearance or malfunctioning that are different from immediately prior observations or experience in operating the equipment must be reported to appropriate DO/bureau security officials for immediate action.

   Security equipment storing classified information that has been opened on a particular day shall not be left unattended where unauthorized persons may gain unescorted access to it. Leaving a security container unattended (and its contents accessible) without either direct visual observation or physical access control by an appropriately cleared individual, no matter how briefly, is a security violation.

d. *Handling the SF 702.* DO/bureau office directors and supervisors shall ensure SF 702 forms are used and may assign the responsibility for checking security containers and annotating the SF 702 to one or more designated duty personnel.

When both sides of the SF 702 are completed, a new SF 702 shall be affixed to the outside of the security container. Retention of completed SF 702 forms is not required by DO offices but may be subject to individual bureau determination at the bureau security officer's discretion.

7. Standard Forms 703, 704, 705 – Classified Document Cover Sheets

Standard Forms 703, 704, and 705 are used to alert personnel that a document, file, or folder to which it is affixed, respectively contains Top Secret, Secret, or Confidential classified information and must be protected. Classified document cover sheets perform the following functions:

(1) Alert users that particular information is classified;

(2) Shield classified documents while being used; and,

(3) Provide protection from unauthorized scrutiny.

a. *Color Coding.* Cover sheets are color-coded orange for Top Secret information, red for Secret information, and blue for Confidential information.

b. *Handling Cover Sheets.* Classified document cover sheets shall be placed on all classified documents or classified folders *when withdrawn from secure storage,* for internal and external transmission and handling/processing.

Individuals preparing, processing, packaging or hand-carrying classified documents are responsible for affixing the appropriate document cover sheet. However, if classified information is delivered or received without the required cover sheet, the recipient is responsible for attaching the proper classified document cover sheet.

Cover sheets should be removed before classified information is securely filed to conserve filing space. Cover sheets should be removed from classified information and recycled prior to destruction of the classified information. Cover sheets are meant to be continually recycled until worn out. To protect the integrity of the color-coding process, cover sheets shall not be photocopied in black/white and put into use. To accommodate emergency use, cover sheets may be reproduced on a color copier. DO/bureau offices are responsible for maintaining their own adequate stock as available through normal supply channels.

c. *Other Cover Sheets.* There are also sensitive compartmented information (SCI), special access program (SAP), and special access required (SAR) cover sheets for

use in protecting such information. These cover sheets are only available through the SSO in Treasury's OIA. Copying SCI, SAP, and SAR information cover sheets outside SSO channels is not authorized.

8. Standard Forms 706, 707, 708 – Labels on Classified Equipment and Media

Standard Forms 706, 707, and 708 are labels used to identify equipment approved for processing classified information at the Top Secret, Secret, or Confidential level, respectively, e.g., copiers approved for classified reproduction, and to identify electronic/magnetic media, e.g., disks/diskettes, removable hard drives, copier hard drives, or similar media containing classified information.

a. *Color-coded Labels.* Labels for classified information in the SF 700 series are color-coded in the same manner as classified document cover sheets:

- Orange for Top Secret (SF 706).
- Red for Secret (SF 707).
- Blue for Confidential (SF 708).
- Purple for "classified but level determination pending" (SF 709).
- Green for "unclassified" (SF 710).
- White "data descriptor" label (SF 711).
- Yellow "SCI" label (SF 712).

In locations where only unclassified information is processed or stored, the use of the green "unclassified" label (SF 710) is optional. However, in environments in which classified and unclassified information is processed or stored, the "unclassified" label must be used to positively identify removable IT media authorized for unclassified use only. Each of these labels is available via national stock number through normal Federal supply channels.

b. *Classified Equipment.* Labels shall be conspicuously placed on classified equipment in a manner that will not interfere with its operation. Once applied, the label shall not be removed. A label to identify a higher classification level may be applied on top of a lower classification level in the event the classification content changes, e.g., from Confidential to Secret. A lower classification label shall never be applied to equipment already containing a higher level of classified information.

c. *Classified Electronic/Magnetic Media.* Employees working with or processing classified information are responsible for properly labeling and controlling electronic/magnetic storage media in their custody. Failure to apply the appropriate security classification label is not a security violation, but it is a

security infraction. If the failure results in improper storage, loss, unauthorized access, or compromise of classified information, however, it would be a violation of established security safeguards.

d. *Removable Electronic/Magnetic Media.* All removable electronic and magnetic media used to process classified information shall be physically labeled with the

highest level of classified information contained therein. The same labeling requirements in 7b above apply to removable electronic/magnetic media.

Removable media shall be physically detached from the processing equipment at the close of business each workday and secured in an appropriate, locked, GSA-approved security container. Removable media will be safeguarded at all times when not otherwise in use and under the constant supervision of a properly cleared DO/bureau employee.

e. *Exception.* An exception to the requirement to physically remove and store such electronic/magnetic items is authorized when the equipment and processing occurs in either of the following areas:

- An approved SCIF.
- A work/storage area that has been specifically approved by the cognizant DO/bureau security official for open-storage of classified information and the area is equipped with minimum security safeguards prescribed by the Treasury Security Manual for classified information.

Such storage shall take into consideration the level of protection required, the nature of security-in-depth within the DO/bureau facility housing the equipment and removable material, and the use of risk-management principles to provide secure, adequate, and cost-effective storage.

9. Standard Forms 709 through 715 – Additional Labels/forms for Classified Equipment, Media and Information Gathering.

SF 709, *Classified Label*, shall be used to identify classified information on electronic/magnetic media when the level of classification has yet to be determined.

SF 710, *Unclassified Label*, shall be used in a mixed environment in which classified and unclassified materials are being processed or stored. This label identifies electronic/magnetic media that specifically contains unclassified information and is an aid in distinguishing amongst those electronic/magnetic containing classified information.

SF 711, *Data Descriptor Label*, shall be used to identify additional safeguarding controls for classified information that is stored or contained on particular electronic/magnetic media.

SF 712, *Classified SCI Label*, shall be used to identify Sensitive Compartmented Information that is stored or contained on particular electronic/magnetic media.

SF 713, *Consent for Access to Records*, shall be used as a release form for Executive Branch investigative and counterintelligence agencies to request financial records or other financial information and consumer reports and in determining eligibility or continued eligibility for access to classified information.

SF 714, *Financial Disclosure Form.*

SF 715, *Declassification Review Tab*, shall be used by agencies working with Federal records under the automatic declassification provision of EO 13526.

10. Treasury Department Forms (TD Fs)

a. *TD F 15-05.1, Security Orientation Acknowledgment.* The TD F 15-05.1 shall be used to document that DO/bureau employees authorized access to classified information have been provided particular security training on how to properly handle and safeguard classified information. Such training is a requirement contemporaneous with the individual's receiving his or her security clearance. The form is also used to document employees receiving refresher and specialized training to maintain current on protective requirements.

b. *TD F 15-05.2, Report of Authorized Classifiers.* The TD F 15-05.2 shall be used to delegate designated DO/bureau officials as original classification authorities at the Top Secret, Secret, or Confidential levels. The form may only be signed by the Secretary (up to Top Secret) or Treasury's Senior Agency Official (SAO) (up to Secret), or someone acting for either official.

c. *TD F 15-05.3, Report of Authorized Downgrading and Declassification Officials.* The TD F 15-05.3 shall be used to designate DO/bureau officials as authorized to downgrade and declassify classified information at a specified level (Top Secret, Secret, or Confidential). The form may only be signed by the Secretary (up to Top Secret) or Treasury's Senior Agency Official (up to Secret), or someone acting for either official.

d. *TD F 15-0.4, Top Secret Document Record.* The TD F 15-05.4 is required to account for all Top Secret classified documents. The form identifies each document's unique Top Secret control number, the date received, additional control notices (if any), number of copies, description, originating agency, document date, disposition (assignment/destruction, etc.) and includes space for remarks.

e. *TD F 15-05.5, Classified Document Certificate of Destruction.* The TD F 15-05.5 is required for documenting destruction of classified information. The form includes space for describing documents that are going to be destroyed, and for the witnessing official and actual destruction official. These individuals must sign their names for accountability/tracking purposes.

f. *TD F 15-05.6, Record of Security Violation.* The TD F 15-05.6 shall be used to initially report a possible security violation. Space is provided for the responsible individual to make a statement as to his or her knowledge of what happened. This is followed by the supervisor's statement with respect to subsequent action. The TD F 15-05.6 becomes a matter of record in those instances where DO/bureau security officials determine the violation to be valid.

g. *TD F 15-05.7, Courier Card.* The TD F 15-05.7 is issued to authorized persons responsible for routinely performing courier duties with respect to the physical transport and securing of classified information within and between DO/bureau and non-Treasury locations. The card is issued as evidence of the bearer's courier authorization and classification level.

h. *TD F 15-05.8, Receipt for Classified Information.* The TD F 15-05.8 is required for receipting purposes, that is, it is used to track and account for classified information exchanged between one or more authorized recipients when accountability is required.

(1) *Requirements.* Receipts for classified information must be used for all Top Secret information but are optional for Secret and Confidential information. The TD F 15-05.8 shall identify both addressee and sender, and describe the document without otherwise revealing any classified information.

(2) *Handling Receipts.* The recipient (or other cleared support staff) shall promptly sign and return the receipt to the sender. The sender shall maintain a record of outstanding receipts for use in subsequent tracer actions if the receipt is not returned within the reasonable time-frame of 30 calendar days. Completed receipts shall be maintained for a 3-year period after which they may be destroyed. No record of the actual destruction of the receipt is required.

Responsible DO/bureau office heads shall determine the administrative procedures required to sufficiently handle the volume of classified information within their organization in conjunction with assistance from DO/bureau security and records management officials.

(3) *Transmitting Several Items at a Time.* Several items may be transmitted to the same addressee with one receipt form. The inclusion of classified

information on the form shall be avoided. For example, if a subject title is classified, an abbreviated short form or title shall be used, as in the first letter of each word in the subject line.

i. *TD F 15-05.9, Reporting of Controlling/Decontrolling Officials.* The TD F 15-05.9 is used to identify those employees authorized to control and/or decontrol sensitive information, as warranted.

j. *TD F 15-05.10, Top Secret Document Record.* The TD F 15-05.10 is used to maintain a record of all persons who handle individual Top Secret documents and including all persons who are orally advised of the content. "Handling" includes signing for, opening, transporting, processing, copying, accountability/tracking and witnessing/destroying Top Secret information.

k. *TD F 15-05.11, Sensitive But Unclassified Document Cover Sheet.* The TD F 15-05.11 is used to protect sensitive information in the same manner as classified document cover sheets.

l. *TD F 15-05.12, Request and Receipt for Courier Card.* The TD F 15-05.12 is to initiate requests for cleared employees and/or contractors to be issued a Treasury courier card authorizing the bearer to transport classified information. See Chapter V, Section 6.

m. *TD F 15-05.13, Classified National Security Information Critical Element for Evaluating Non-SES, Original Classification Authorities, Security Managers/Specialists and Employees whose duties involve the Creation or Handling of Classified Information.* The TD F 15-05.13 provides a means for evaluating affected employees annual performance contract or evaluation with respect to classified information as required by Executive Order 13526.

n. *TD F 15-05.14, Request and Receipt for Official Credential.* The TD F 15-05.14 is used to initiate requests for those officials requiring evidence of the bearer's authority when contacting the public and/or conducting U.S. Government business with Federal, State, local or foreign officials as authorized by law, statute or Treasury/bureau regulation. See Chapter V, Section 5.

o. *TD F 15-05.15, Security Debriefing Information.* The TD F 15-05.15 is a handout provided for formerly cleared and departing employees/contractors advising them of their continued responsibilities to safeguard classified information based on having signed the Classified Information Non-disclosure Agreement, Standard Form 312.

p. *TD F 15-05.16, Request for After-hours Access to the Main Treasury Complex.* DO use only.

q. *TD F 15-05.17A and B, Treasury Department Credential.* DO use only.

r. *TD F 15-05.1888, Main Treasury Complex Work Order/Pass Application.* DO use only.

s. *TD F 15-05.19, Inadvertent Disclosure Briefing and Agreement.* The TD F 15-05.19 is used when classified information has been unintentionally and/or inadvertently discussed with, viewed or exposed to personnel during their officially assigned duties. It includes the employee's agreement to safeguard the information in the same fashion as the SF 312. The form is used to mitigate damage with un-cleared employees or those exposed to classified information above their security clearance level.

t. *TD F 15-05.20, Classified Meeting in Progress Sign.* To be posted on doors when classified meetings are being held to provide notice thereof (and limit access to appropriate attendees).

u. *TD F 15-05.21, Report of Security Incident* (for Computer Data Spills). Form to report pertinent information relating to spills of classified information on unclassified systems which includes desktops, laptops, blackberries, etc., and including improperly handled/processing on the Treasury Secure Data Network and Treasury Foreign Intelligence Network.

11. Open/Closed or Locked/Unlocked Signs

Reversible "Open/Closed" or "Locked/Unlocked" signs shall be used on security equipment storing classified information. Such signs help to remind DO/bureau employees whether a security container is open (unlocked) or closed (locked). The signs augment internal security practices to further reduce the possibility of a security violation. They are available through commercial supply channels and may be magnetic or constructed of rigid cardboard and are intended to be reused.

12. Supply of Forms

DO/bureaus can obtain SF 311 at http://www.gsa.gov/forms/pdf_files/sf311.pdf listed on GSA's website under *Standard Forms*. Additionally, GSA's website at www.gsa.gov/Portal/gsa/ep/formslibrary.do may also be queried to obtain ISOO prescribed forms.

Several of the Treasury Department forms in this section can be obtained from the Office of Security Programs (OSP) website at http://intranet.treas.gov/security/forms/ or otherwise through normal DO/bureau printing procurement or on-site printing channels.

Chapter III **Information Security Program Reports** Updated
Section 4 5/15/14

1. Introduction

This section establishes requirements, responsibilities, and time frames for collecting and reporting statistical data, cost data, and related information on each DO/bureau reporting component's information security program. This includes reports required by the Information Security Oversight Office (ISOO) as well as the Department of the Treasury, Office of Security Programs.

2. Background

The ISOO is the government-wide agency tasked with advising the President on the status of each individual agency's information security program.

The information security program is primarily based on Executive Order (EO) 13526. ISOO requires Federal agencies and departments handling classified information to report statistical data and security classification-related cost data every year about their program. All Treasury/bureau-wide data is consolidated by Treasury's Office of Security Programs (OSP) and forwarded to the ISOO.

NOTE: The Office of Special Security Programs collates reporting data on SCI original and derivative classification decisions that is provided to the OSP.

3. ISOO Information Security Program Reports

a. *Agency Security Classification Management Program Data, Standard Form (SF) 311* includes statistical data on the: (1) number of officials authorized to originally classify; (2) annual volume (and levels) of original and derivative classification decisions; (3) status of new, carried-over, and mandatory declassification review appeals; (4) number of pages subject to automatic declassification and systematic review; (5) number of internal oversight reviews, (6) number f security classification guides in current use; and (7) explanatory comments. This form, revised July 2010, is at http://thegreen.treas.gov/policies/Forms1/Agency%20Security%20Classification%20Management%20Program%20Data.pdf. Earlier versions of the SF 311 may NOT be used.

(1) *Time Frame*. DO/bureau reporting components shall provide their statistical data to OSP on SF 311 no later than November 1st of each year. The reporting period covers a 12-month time frame from October 1st through September 30th. The November 15th due-date on the top of the SF 311 applies to Federal

agencies and departments. DO/bureau reports shall not be sent to ISOO.

(2) *Instructions.* DO/bureau reporting components (and their clients) shall maintain a "classified chronological file" or comparable system to account for all original and derivative classification during each reporting period. Whenever a classified document is created, a hard copy (paper) should be placed in a dedicated "chron file" and secured in a General Services Administration (GSA)-approved security container. When the formal data call is received, the "chron file" contents are counted and the data is entered on the SF 311 where it applies. The "chron file" can be maintained centrally, by division, office, or individual, at the discretion of each reporting activity to ensure efficiency of service.

Classified information processed and transmitted via secure email shall also be accounted for when the email is equivalent to a finalized classified document or official policy-level decision/position. The statistical totals by level of classification and original or derivative classification shall be added to the number of hard copy paper documents. The volume of email messages equivalent to telephone conversations used to exchange information/options shall not be included in the accounting of classified documents.

Any additional instructions for completing the SF 311 issued by the ISOO will be disseminated by the OSP to reporting DO/bureaus.

b. *Security Classification-related Cost Data* include: (1) estimates of budgetary funding for personnel security, physical security, information security (including classification management, declassification, information systems security and miscellaneous costs (Operations Security (OPSEC) and Technical Security Countermeasures (TSCM)), professional education, training and awareness; (2) security management, oversight and planning; and, (3) unique items, as warranted.

Cost data is reported in actual dollars by fiscal year on a security costs estimates display format that was developed by ISOO.

(1) *Time Frames.* The due date for reporting cost data varies at ISOO's discretion (generally Executive Branch departments and agencies are notified by February 1st and are expected to respond by April 15th). DO/bureau components will be advised of the due date for this report by the OSP.

(2) *Instructions.* Instructions prepared by ISOO are normally in memo format and will be disseminated by the OSP to reporting DO/bureau offices.

4. Treasury Information Security Reports

The OSP reports are in addition to required ISOO reports. Each of these Treasury forms may be obtained from OSP's website at http://intranet.treas.gov/security/forms/.

a. *Report of Authorized Classifiers* - Treasury Department Form (TD F) 15-05.2, shall be used to identify DO/bureau officials whose duties require designation as an original classifier for national security information. Officials are identified by name, position title, and level of classification authority.

Persons and positions so identified are exclusive of those identified in Treasury Order (TO) 105-19. All delegations of authorized classifiers shall be in writing on TD F 15-05.2 and forwarded to OSP for signature by the Secretary (if delegating original Top Secret classification authority) or the Senior Agency Official (SAO), if delegating original Secret or Confidential classification authority).

(1) *Time Frame.* DO/bureau reporting components shall use TD F 15-05.2 in conjunction with their annual submission of the SF 311 report to the OSP. Such reports remain valid until cancelled by succeeding TD Fs 15-05.2 each year.

(2) *Instructions.* Instructions for completing TD F 15-05.2 are on the reverse side of the form. All persons so identified must attend mandatory original classification authority training conducted as required by EO 13526 on an annual basis. This training is to ensure designated officials are proficient in processing, marking, and safeguarding classified information.

b. *Report of Authorized Downgrading and Declassification Officials,* TD F 15-05.3, shall be used to identify DO/bureau officials, by name, position title, and level of authority whose duties warrant being designated to downgrade and declassify national security information.

(1) *Time Frame.* DO/bureau reporting components shall use TD F 15-05.3 in conjunction with their annual submission of the SF 311 report to the OSP. Such reports remain valid until cancelled by succeeding TD F 15-05.3 each year.

(2) *Instructions.* Instructions for completing TD F 15-05.3 are on the reverse side of the form. Persons so identified must have current jurisdiction and control over: (1) classified documents subject to mandatory review, automatic declassification, or systematic declassification review, under EO 13526 or, (2) related examinations of classified records. Persons and positions so identified are exclusive of those identified in TO 105-19. All delegations of authorized classifiers shall be in writing on TD F 15-05.3 and forwarded to Treasury's OSP for signature by the Secretary or SAO. All persons so identified must attend mandatory training conducted or

approved by the Director, OSP, and/or bureau security officials on an annual basis to ensure designated officials are proficient in safeguarding classified information and downgrading and declassifying national security information.

c. *Report of Controlling/Decontrolling Officials,* TD F 15-05.9, is now optional. DO/bureau reporting components that restrict designation of sensitive information to specifically authorized persons shall use TD F 15-05.9 to identify such officials, by name, position title, and identify or any other category of information authorized by law, statute or regulation warranting control/decontrol.

(1) DO/bureau reporting components shall use TD F 15-05.9, in conjunction with their annual submission of the SF 311 report to the OSP. Such reports remain valid until cancelled by succeeding TD Fs 15-05.9 each year.

(2) *Instructions.* Instructions for completing TD F 15-05.9 are on the reverse side of the form. All persons so identified must attend appropriate training conducted or approved by bureau security officials to ensure designated officials are proficient in safeguarding sensitive information authorized by law, statute or regulation. The form should be signed by the person responsible for their bureau's information security program and forwarded to Treasury's OSP.

Chapter III Section 5 **Original and Derivative Classification** Updated 6/20/14

1. Introduction

Original classification is the determination by an authorized official that information within specifically designated categories requires protection against unauthorized disclosure in the interests of national security. Further, the above disclosure could reasonably be expected to result in a degree of damage to the national security, including defense against transnational terrorism that the original classification authority is able to identify or describe.

Derivative classification is the restatement of existing classified information by persons who reproduce, extract, or summarize, or apply classification markings derived from source material or as directed by a classification guide.

The basis for classification is Executive Order (EO) 13526, dated December 29, 2009, *Classified National Security Information* and Information Security Oversight Office (ISOO) implementing directive contained in 32 CFR Part 2001.

2. Original Classification and Authority Delegations

"Original" classification is the initial determination that information requires protection against unauthorized disclosure in the national interest. This is coupled with a classification designation signifying the level of required protection as determined by an Original Classification Authority (OCA). Departmental Offices (DO)/bureau OCA officials are identified in Treasury Order (TO) 105-19, *Delegation of Original Classification Authority; Requirements for Declassification and Downgrading.* Additional OCAs require written designation by the Secretary of the Treasury (at the Top Secret, Secret and Confidential levels) or by Treasury's Senior Agency Official (SAO) (at the Secret and Confidential levels). Identification and designation of such OCA officials shall be coordinated by Treasury's Office of Security Programs (OSP).

According to the Office of the Director of National Intelligence with respect to national intelligence, a separate OCA designation for "dual-hatted" Treasury officials is unnecessary provided the official exercises OCA authority consistent with direction, guidance and all other Presidential Directives, Executive Orders and legal authorities for national intelligence. Additionally, exercise of the authority is limited to only that information falling within the OCA's scope of authority requiring protection. It does not apply to information within other organizations where a classification guide or original classification decision has already been made.

3. Derivative Classification and Authority

"Derivative" classification means incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification may be exercised by any DO/bureau employee, consultant or contractor (under the National Industrial Security Program (NISP)) with a security clearance. The basis for derivative classification actions involves use of one or more of the following types of information:

- Existing classified source document.
- Approved classification guide.
- Classified communication, e.g., information provided orally via secure phone or obtained/discussed during a classified meeting.

4. Classification Levels

Classified information, also known as classified National Security Information (NSI) is information that has been determined pursuant to EO 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Classified information shall be identified by one of the following three levels: Top Secret, Secret or Confidential.

- Top Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.

- Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.

- Confidential shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe.

5. Classification Standards

In order for information to be properly classified it must be:

- Designated (as classified) by an OCA.
- Owned by, produced by, or for, or under the control of the U.S. Government.
- Be within one or more of the classification categories in Section 1.4, EO 13526 in

paragraph 6 below.

- The OCA must determine that unauthorized disclosure of the information could reasonably be expected to result in damage to the national security (including defense against transnational terrorism) and the OCA is also able to identify or describe the damage.

Significant Doubt. If there is significant doubt about the need to classify information, it shall not be classified. However, when a DO/bureau employee, government contractor, licensee, certificate holder, or grantee who does not have original classification authority creates information believed by that person to require classification, the information shall be tentatively marked as classified or indicate a classification decision is pending and be protected in a manner consistent with the EO and its implementing directives. The information shall be transmitted as if it was duly classified and promptly provided to the appropriate DO/bureau official with subject matter interest (having original classification authority) with respect to this particular information. The DO/bureau official shall decide within 30 days whether or not to classify this information. The information will then be marked accordingly to reflect the official's decision.

6. Classification Categories

Information shall not be classified unless it concerns one or more of the following; those in bold text indicative of DO/bureau rationale for classification:

a. Military plans, weapons systems, or operations.

b. Foreign government information.

c. Intelligence activities (including covert action), intelligence sources or methods or cryptology.

d. Foreign relations or foreign activities of the United States, including confidential sources.

e. Scientific, technological, or economic matters relating to the national security.

f. United States Government programs for safeguarding nuclear materials or facilities.

g. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.

h. Development, production, or use of weapons of mass destruction.

7. Classification within a Treasury Context

DO/bureau officials may consider U.S. economic viability/well-being, market sensitivity, U.S. global competitiveness, tracking terrorist assets/financial crimes as rationale for classification. See Treasury's Security Classification Guide at http://thegreen.treas.gov/policies/Resources/Treasury%20Security%20Classification%20Guide.pdf .

8. Classification in Context of Related Information

Certain information that would otherwise be unclassified might require classification when combined or associated with other unclassified, sensitive, or classified information. Such classification on an aggregate basis (also known as mosaic classification) shall be supported by a written explanation that, at a minimum, is maintained with the file or referenced on the record copy of the information. This could apply when the compilation reveals an additional association or relationship that meets the requirement for classification under EO 13526 and/or is not otherwise revealed in the individual items of information.

9. Duration of Classification and Automatic Declassification

a. When information is originally classified, the OCA is responsible for establishing a specific date or event for declassification based upon the duration of the national security sensitivity of the information. Upon that date or event being reached, the information shall be automatically declassified. The following sequence shall be followed in setting the declassification time frame:

b. The OCA shall set a date or event ten years from the date of original classification that coincides with the lapse of the information's national security sensitivity unless he/she otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the original decision. OCAs are encouraged to apply earlier dates/events for declassification as befits particular information when a shorter time frame is warranted. Classification dates may be written out (as in September 11, 2010) or identified numerically; for example, 9/11/10 or based on (YYYYMMDD) as in 20100911.

c. Within DO (except for the Office of Intelligence and Analysis and its predecessor, the Office of Intelligence Support) and all bureaus (except the United States Mint (with respect to the gold bullion depository at Fort Knox and the Bureau of Engraving and Printing), classified information reaching 25 years of age that was originated by DO and these two bureaus is automatically declassified. Classified information originally classified by those identified above shall be referred to these organizations for declassification.

10. Classified Addendums or Attachments

OCAs shall use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document; this is for ease of information sharing and further safeguarding. This practice might involve including short text of a few paragraphs as a classified attachment. Whether a classified addendum/attachment is developed and used, it must feature the same overall, paragraph/portion markings and declassification instructions that identify a classified document.

11. Changes in Classification Markings

Changes in classification markings may be made when the declassification date/event is altered or when the classification level is downgraded (or upgraded) or declassified, as the case may be. Whenever such a change is made, all holders of records shall be promptly notified as practicable. Holders shall alter the markings on their copy of the information to conform to the change and cite the DO/bureau authority for it. Note that only an Original Classification Authority is authorized to extend the duration of DO/bureau classified information up to a maximum of 25 years from its date of origin. Items withdrawn from file collections of classified records for purposes other than transfer to alternate storage shall be properly marked in accordance with the change notice(s). If remarking large quantities of information is unduly burdensome, the holder must attach a change of classification notice to the storage unit in lieu of the marking action otherwise required.

12. Omitted Classification Markings

Information contained in unmarked records, Presidential or related materials and which: (1) pertain to the national defense or foreign relations of the United States; and, (2) has been maintained and protected as classified information under prior Orders, shall continue to be treated as classified information under EO 13526, and is subject to its provisions regarding declassification. Such information shall be considered as classified despite the omission of other required markings. Whenever such information is used as a source for derivative classification or is reviewed for possible declassification, holders shall coordinate with the appropriate OCA to ensure any omitted markings are applied to the document.

13. Classification Guides

A classification guide is a documentary form of guidance issued by an OCA identifying elements of information regarding a specific subject that must be classified and establishing the level and duration of classification for each such element. Guides assist document drafters in determining what types and categories of information have already been classified and what information is classifiable in a national security sense. Each guide is a tool for users to facilitate the proper and uniform derivative classification of information. Each classification guide constitutes pre-approval by one or more OCAs

that specific information should be classified.

Guides are meant to facilitate standardization when classified information is incorporated, paraphrased, restated, or generated in new form by DO/bureau derivative classifiers (any employee with a security clearance). If the derivative classifier is of the opinion that their action(s) in transposing information or in conjunction with other material has changed the level (or altered the basis for) classification, they shall consult with an official of the originating DO/bureau who has the authority to upgrade, downgrade or declassify the information for a final decision. Such consultation shall ensure adequate protection of the information while the determination is being made and thereafter for information that remains classified.

Classification guides may be prepared by individual DO/bureau components or for individual and specialized projects/programs. Guides are meant to have the widest internal dissemination necessary for efficient use. Copies of all DO/bureau classification guides, including any guides that are classified at the Top Secret, Secret, or Confidential level, shall be provided to the Director, OSP. These classification guides are subject to review by appropriately cleared OSP employees to ensure compliance with EO 13526. In a change to Standard Form 311 (Agency Security Classification Program Data), revised July 2010, reporting officials are required to identify the number of classification guides created and currently in use.

Each classification guide must be approved in writing by an OCA identified in TO 105-19, and it must also identify one or more points-of-contact to respond to questions or inquiries about the particular guide. Guides are meant to be living documents and shall be reviewed and updated periodically based on a comprehensive review. Classification guidance reviews shall include an evaluation of classified information to determine if it meets the standards for classification. Participation shall also include original classification authorities and DO/bureau subject matter experts to ensure a broad range of perspectives. Reviews shall also capture information following any new, original classification decisions made by an OCA that are not otherwise identified in the guide. At a minimum, a classification guide shall identify the:

- Reason to classify from Section 1.4 (a-h), EO 13526 (see paragraph 6, above).
- Identification of the subject matter of the guide.
- The OCA authority by name and position or personal identifier.
- DO/bureau point of contact for questions regarding the guide.
- Date of issuance or last review.
- State the precise elements of information to be protected.
- Level of classification to be applied to each item description, and when useful the elements of information that are unclassified.
- Any special handling caveats, as applicable.
- Declassification date or event timeframe or Interagency Security Classification Appeals Panel-approved exemption. (See paragraph 16 below).

14. Identification and Markings

a. *Classification Level.* The markings Top Secret, Secret, and Confidential shall be used to indicate the following:

- Information requiring protection as classified EO 13526.
- The highest level of classification contained in a document.
- The classification level of each page.
- In abbreviated form, the classification of each paragraph or portion of a document, including the subject line, i.e., (TS) for Top Secret, (S) for Secret, (C) for Confidential, (U) for Unclassified and (SBU) for sensitive information.

NOTE: Classification Management guidance for SCI material may also be found in:

- CAPCO, *Intelligence Community Classification and Control Markings Implementation Manual.*
- ICD 710, *Classification and Control Markings System.*

b. *Overall Marking.* The highest level of classification of information in a document shall be marked in such way to clearly distinguish it from the text. Markings shall appear at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first and last pages bearing text, and on the outside of the back cover (if any).

c. *Page Marking.* Each interior page of a classified document shall be marked at the top and bottom, either according to the highest classification of the content of the pages, including the designation "UNCLASSIFIED" when it is applicable, or with the highest overall classification of the document.

d. *Subject Line, Paragraph or Portion Marking.* The subject line shall identify whether it is classified (and level thereof) or whether it is unclassified. Each paragraph/portion of a document, including subject lines, shall be marked with a parenthetical designation immediately preceding the text to which it applies.

e. *"Classified by" Marking and Reason.* At the time of original classification the OCA's identity, by name and title, shall be indicated on the face of each classified document and applied to other classified media in an appropriate manner. The concise reason(s) for each original classification (from Section 1.4 (a-h)) EO 13526, shall be identified, along with a declassification date or event.

The following marking shall appear on the bottom, right hand side of the first or cover page of each originally classified document; including classified information in electronic format, unless specific information would itself reveal additional classified information.

Classified by:	OCA's name and title
Reason:	One or more reasons from Section 1.4 (a-h) EO 13526 or OCA's statement as to why the document is classified
Declassify on:	Declassification date (in alpha-numeric or YYYYMMDD format) or declassification event

f. *"Classified by" Marking and "Derived from" Marking.* At the time of derivative classification the employee's, consultant's, or contractor's identity (by name or personal identifier and office) shall be indicated on bottom (right-hand) face of each classified document and also applied onto other classified media in an appropriate manner.

(1) Information derived from one or more existing classified source documents, or classification guides, or classified communication (information provided orally via secure phone or obtained/discussed during a classified meeting) shall be indicated on the bottom (right-hand) face of each classified document and applied to other classified media in an appropriate manner. When more than one source is used, the "*Derived from*" line shall indicate "multiple sources." A listing of source documents shall be maintained with the official file record of the document or be maintained electronically if the official DO/bureau file records are kept in that format.

(2) Normally, the declassification date or event from the classified source document shall be carried over to the derivatively classified document. If there is more than one source, the date or event allowing the information to remain classified furthest into the future shall be used for declassification purposes. When using an approved classification guide, DO/bureau employees, consultants or contractor personnel shall apply the date or event for declassification as instructed by the guide. Documents that were derivatively classified based on a classified communication shall apply the date or event for declassification consistent with the discussion within the prescribed 10 to maximum 25-year timeframe.

The following marking shall appear on the bottom, (right-hand) of the first or cover page of each derivatively classified document derived from an existing classified source document, classification guide or classified meeting/discussion; this includes classified information in electronic format.

Classified by:	DO/bureau employee's name and office
Derived from:	Source document or classification guide or secure meeting/discussion
Declassify on:	Declassification date or event (from source, guide, or meeting/discussion)

The following marking shall appear on the bottom (right-hand) of the first or cover page of each derivatively classified document derived from multiple sources.

Classified by:	DO/bureau employee's name and office
Derived from:	Multiple sources
Declassify on:	Declassification date or event (from source with furthest future time frame)

15. Obsolete Marking Terms

The following terms are no longer useable on originally classified documents but may be cited when the source document is so marked. In such instances the date of the source bearing such marking must be included on the "*Classified by*" line of derivatively classified documents; the previous "*Derived by*" is no longer valid. These terms include, "Originating Agency's Determination Required", also known as "OADR", "Impossible to Determine" and "X-1" through "X-8" exemption categories from the 10-year maximum duration of classification rule. The term "Entire Text Classified" shall not be used in lieu of identifying the level of classification of individual paragraphs/portions or subject lines on classified documents.

16. Citation of Exemption Categories and Markings

If an OCA is classifying information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, the duration shall be up to a maximum of 75 years and be designated by the following marking, "50X1-HUM". Use of other exemption markings requires pre-approval by the Interagency Security Classification Appeals Panel (ISCAP) through the ISOO. DO/bureau requests for authorization to use exemptions must be in writing and coordinated with the Director, OSP.

17. Electronically Processed Document Markings

Classified documents generated electronically on specifically-approved IT equipment or systems, including cables or other message traffic, might be marked automatically by the system software. IT systems for classified processing might prompt the user to input specific categories of information: (1) classification level; (2) EO 13526; (3) declassification date, etc., name/alphanumeric identifier of original/derivative classifiers and/or title; (4) office of origin; and/or, (5) reason(s) for classification and any applicable exemptions. Despite system prompts identifying these markings, these same markings (including the declassification instructions) must appear in classified attachments. Where system prompts do not identify the classification of individual portions, paragraphs, or bullets, etc, employees are responsible for ensuring the appearance on classified email they generate.

Classifiers must ensure the application of required markings and declassification instructions assigned to particular information remain constant – especially on email streams of classified information. Whenever the required markings cannot be affixed to specific classified information or materials, originators shall provide holders or recipients with written instructions for protecting the information. Markings shall always be uniformly and conspicuously applied to leave no doubt about the classified status of information, the level of required protection and the duration thereof.

Removable IT media shall bear external labels indicating the security classification level of the information and any associated security markings, such as handling caveats or dissemination controls, as applicable. Examples of such media include, but are not necessarily limited to disks, diskettes, disk packs, magnetic cartridges/cassettes; U.S. Government authorized USB, flash/thumb drives and removal hard drives on copiers. Security classification labels are standardized forms (SF 706, 707 and 708), color-coded in the same manner as classified document cover sheets; orange for Top Secret (SF 706), red for Secret (SF 707), blue for Confidential (SF 708). There are also purple for "classified but level pending (SF 709), green for "unclassified" (SF 710) and white "data descriptor" (SF 711) color-coded labels.

In locations where only unclassified information is processed or stored, the use of the green "unclassified" label (SF 710) is optional. However, in environments in which classified and unclassified information is processed or stored, the "unclassified" label must be used to positively identify removable IT media authorized for unclassified use only. Each of these labels is available via national stock number through normal Federal supply channels.

18. Unofficial Publication or Disclosure

Following an inadvertent or unauthorized disclosure or publication of information identical or similar to information that has been classified in accordance with EO 13526 or predecessor Orders, a determination shall be made of the degree of damage to the national security, the need for continued classification, and, in coordination with the DO/bureau organization or outside agency in which the disclosure occurred, what action(s) must be taken to prevent similar occurrences. Classified information shall not be automatically declassified as a result of an unauthorized disclosure as for example, in the news media. Prior to public release, all declassified records shall be appropriately marked to reflect the declassified status of the information.

19. Limits to Classification, Over-Classification and Reclassification

a. *Limitations*. Markings other than Top Secret, Secret, and Confidential shall not be used to identify classified information. No other terms or phrases such as "Secret/Sensitive" or "Administratively Confidential" shall be used in conjunction with these markings to identify classified information.

b. *Over-classification.* In no case shall information be classified to: (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or, (4) prevent or delay the release of information that does not require protection in the interest of national security. Information shall only be classified when it meets established criteria for protecting the national security.

Original and derivative classifiers are responsible for properly marking classified information they generate and ensuring instances of over-classification are avoided. This includes reducing the length of email strings and not repeatedly sending classified information already provided. Acknowledgments of receipt, referrals for information only and responses that do not contain classified shall be contained in new, unclassified emails. Additionally, if there are different levels of classification among paragraphs, sub-paragraphs, bullets and sub-bullets all segments shall be portion marked separately in order to avoid over-classification of any one segment. See Chapter III, Section 20, regarding challenges regarding over-classification or incorrect classification.

c. *Reclassification.* Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following:

- The reclassification action is personally approved in writing by the Secretary of the Treasury based on a document-by-document determination by that official that reclassification is required to prevent significant and demonstrable damage to the national security;
- The information may be reasonably recovered without bring undue attention to it.
- The reclassification action is reported promptly by the Director, OSP to the Director, ISOO and the Assistant to the President for National Security Affairs (National Security Advisor).
- For documents in the physical and legal custody of the National Archives and Records Administration that have been available for public use, the Secretary of the Treasury has, after making the above determination, notified the Archivist of the United States, who shall suspend public access pending approval of the reclassification action by the Director, ISOO. Any such decision by the Director, ISOO, may be appealed by the Secretary of the Treasury to the National Security Advisor and public access shall remain suspended pending a prompt decision on the appeal.

20. Reclassification after Receipt of a FOIA Request

Information that has not previously been disclosed to the public under proper authority

may be classified or reclassified after a request has been received by DO/bureaus under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act (44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of EO 13526 if such classification meets the requirements of the EO and is accomplished on a document-by-document basis with the personal participation or under the direction of the Secretary of the Treasury, the Deputy Secretary, or the Senior Agency Official designated under section 5.4 of the EO. Any such reclassification activity shall be coordinated with the participation of the Director, OSP

21. Record Requirements and Chronological Files

Every original and derivative classification action must be accounted for annually and reported to Treasury's OSP for consolidation into an overall report for the ISOO at the end of each fiscal year. OSP may request additional information from DO/bureau components to fulfill its obligations with respect to the Department's information security program.

Employees, consultants and contractor personnel are responsible for keeping a record each fiscal year of all original and derivative classification decisions on Standard Form 311. This accounting includes classified email (equivalent to final documents or position papers) prepared on equipment approved for processing classified information. An effective way to account for the volume of classified documents is to establish a classified chronological file. Whenever a final document (or equivalent classified email message is created) a hard paper copy is inserted in the dedicated chronological file. That file is properly marked with the level of the classified content and stored in a General Services Administration (GSA)-approved security container. When the OSP data call is sent out to report that year's information security statistics, the file documents are counted by original/derivative classification and respective classification levels. Retention of the file after its contents are accounted for is at the discretion of the file custodian; the key is to use this collection methodology throughout the year. Chronological files might be maintained by individual employee, supervisor, office, division, section, etc., or centralized as befits the efficiency of the DO/bureau.

22 Demonstrable and Continuing Need

OSP is responsible for monitoring the exercise of original classification activity throughout the entire Department. Monitoring includes recommending any additions or deletions of designated officials to be identified and or removed from TO 105-19. Recommendations for changes shall be based on the demonstrable and continuing need of the official to exercise original classification authority (including specialized or ad hoc projects warranting classification for national security reasons) and as reported on Standard Form 311 annually. If, after reviewing and evaluating these reports, OSP (in consultation with the affected OCA) determines there is no demonstrated or continuing need to exercise the authority, the Department's SAO is required to take appropriate action (in liaison with the Secretary) to reduce the authority. Such action might include

relinquishing authority to originally classify where the SAO finds no classification activity is taking place.

23. Reasonable Doubt

If there is significant doubt about the need to classify information, it shall not be classified. However, when there is still reasonable doubt, it shall be safeguarded as if it were at least Confidential, pending a determination by an OCA. When such determination affirms the initial protection, the information will be marked to reflect its final classified status in compliance with the Treasury Security Manual. When such determination results in a decision by an OCA that the information does not warrant classification, the tentative Confidential markings will be obliterated. OCA decisions shall be final.

24. Transmittal Documents

A transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal itself is unclassified, the document shall be marked as either:

- *Unclassified When Classified Enclosure* (for letters), *is Detached;* or
- *Unclassified When Classified Attachment* (for memos*), is Detached.*

Where the transmittal document itself is classified, the document shall be marked as either:

- *Upon Removal of Enclosure* (for letters) *this Document is Classified* (fill in appropriate level); or
- *Upon Removal of Attachment* (for memos) *this Document is Classified* (fill in appropriate level).

25. Foreign Government Information (FGI)

The unauthorized disclosure of foreign government information is presumed to cause damage to the national security. Foreign government information is information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence. It also includes information produced by the U.S. Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring the information, the arrangement, or both, is to be held in confidence

Documents that contain foreign government information shall either retain its original

foreign classification marking, the phrase, "*This Document Contains (indicate country of origin) Information*", or a marking that otherwise indicates that the information is from a foreign government or international organization of governments or any element thereof.

If the specific identity of the foreign government must be concealed, the document shall be marked "*This Document Contains Foreign Government Information*" and pertinent portions shall be marked "*FGI*" together with the classification level, for example, "*(FGI-S (*for Secret*)) or FGI-C* (for Confidential))". In such cases a separate record that identifies the foreign government shall be maintained in order to facilitate subsequent declassification actions.

DO/bureaus shall indicate the portions of documents that contain foreign government and classification level using accepted country code standards, for example (Country code-S) or (County code-C). See Chapter III, Section 8 for the listing of country codes for marking classified information.

If the fact that such material is foreign government information must be concealed given the relationship, understanding, or expectation with the foreign government or international organization of governments providing the information that it is to be held in confidence, the above markings shall not be used and the document marked as if it were wholly of U.S. origin. When classified records are transferred to NARA for storage or archival purposes, the documentation shall, at a minimum, identify the boxes that contain FGI.

26. Restricted Data or Formerly Restricted Data

"Restricted Data" (RD) is information dealing with the design, manufacture, or utilization of atomic weapons, production of special nuclear material, or use of special nuclear material in the production of energy. "Formerly Restricted Data" (FRD) is classified information that has been removed from the "restricted data" category but still remains classified and relates primarily to the military application of atomic weapons. Release of RD or FRD held by DO/bureau components requires coordination with the Department of Energy (DOE) and/or the Department of Defense (DOD). RD or FRD shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended, as prescribed by DOE and/or DOD.

27. Classified Working Papers

A working paper is any document or material (regardless of media) expected to be revised as a finalized product for either information retention or dissemination purposes. Working papers containing classified information shall be dated when created, marked with the highest level of classified information it contains and include portion/paragraph, subject line markings to indicate those sections that are classified (the level thereof) and those parts which are unclassified, and declassification instructions.

Classified working papers and earlier iterations may be destroyed, at the discretion of the originator, so long as the destruction process is in compliance with security requirements for classified information. Working papers shall be protected, controlled, and marked in the same manner as finalized documents whenever: (1) released by the originator outside of DO/bureaus; (2) retained beyond 180 days of origin; or, (3) permanently filed.

28. Bulky Material, Equipment and Facilities

Bulky material, equipment and facilities, etc., shall be clearly identified in a manner leaving no doubt about: (1) the classification status of the material, equipment or facility; and, (2) the level of required protection and duration of classification. Only when this information would itself reveal classified information may the specific identification be omitted.

Chapter III
Section 6

Required Markings on Treasury Classified Information

Updated
6/17/11

1. Introduction

Basic markings used to identify classified information are addressed in Executive Order (EO) 13526, *Classified National Security Information*, dated December 29, 2009 and Information Security Oversight Office (ISOO) Directive 1, dated June 28, 2010. Proper markings must be applied to all classified Departmental Offices (DO)/bureau documents, cables, messages, and electronically formatted items. System prompts may automatically apply the required overall, paragraph/portion and classified by markings on originally or derivatively classified information. However, if DO/bureau systems do not, the document creators are responsible for doing so in the body of the text.

For additional marking guidance see the on-line ISOO *Marking Booklet* at http://www.archives.gov/isoo/training/marking_book_update.pdf. If these markings cannot be affixed to specific classified information or material, the originator shall provide holders or recipients of the classified information with written instructions for protecting the information. In cases where classified information in an electronic environment cannot be marked is such manner to maintain traceability of classification decisions to the original classification authority, a warning shall be applied to alert users that the information may not be used as a source for derivative classification and providing a point of contact and instructions for users to receive further guidance on the use and classification of the information. Markings are intended to be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.

2. Identifying Classified Information

a. *Required Markings.* For both originally and derivatively classified documents, classification markings shall appear on various parts of hard-copy paper documents and electronically formatted documents such as e-mail. The parts of a document that are marked and the markings are described below.

(1) *Overall Document, Covers, Title Page.* The overall marking is determined by the highest classification level of any one portion within the document. The highest overall level shall appear at the top and bottom of the front/back covers (if any), on the title page (if any) and the first page of each classified document. This marking shall be clearly distinguished from the written text. For example, if a document contains information marked "Secret" and other information marked "Confidential," the highest overall marking will be "Secret."

(2) *Interior Pages.* Each interior page shall be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation "Unclassified" when applicable, or with the highest overall classification of the document.

(3) *Subject Line.* Subject lines shall be portion marked to reflect the sensitivity of the information in the subject line and shall not reflect any classification markings for the content or attachments. This marking shall appear at the beginning of the subject line.

(4) *Paragraph or Portion Markings.* Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. The latter generally includes portions not meeting the standards for classification or otherwise determined to be sensitive. The following parenthetical symbol shall be used to indicate classified, unclassified or sensitive by placing it immediately preceding the portion to which it applies:

(TS) for Top Secret
(S) for Secret
(C) for Confidential
(U) for Unclassified
(SBU) for sensitive information

Markings other than "Top Secret", "Secret", and "Confidential" shall not be used to identify classified national security information.

In cases where portions are segmented such as paragraphs, subparagraphs, bullets, and sub-bullets and the classification level is the same throughout, it is sufficient to put only one portion marking at the beginning of the main paragraph or main bullet. If there are different levels of classification among these segments, than all segments shall be portion marked separately in order to avoid over-classification of any one segment.

If the information contained in a subparagraph or sub-bullet is a higher level of classification than its parent paragraph or parent, this does not make the parent classified at that same level. Each portion shall reflect the classification level of that individual portion and not any other portions.

b. *Date of Origin.* The date of origin of the document shall be indicated in a manner that is immediately apparent.

c. *Waivers.* Only the Secretary of the Treasury or the Department's Senior Agency Official (SAO) may request a waiver from the portion-marking requirement (from the Information Security Oversight Office (ISOO)) for a specific category of information; the waiver must include reasons why the benefits of portion marking are outweighed by other factors and demonstrate that the requested waiver will not create impediments to information sharing. Statements citing administration burden alone are not sufficient grounds to support a waiver.

Requests from Treasury's Office of Intelligence and Analysis shall include a statement of support from the Director of National Intelligence or his or her designee. All waiver requests from the portion marking requirements will be coordinated through the Director, Office of Security Programs (OSP). Any approved portion marking waiver will be temporary with specific expiration dates. Documents not portion marked, based on an ISOO-approved waiver must contain a warning statement that it may not be used as a source for derivative classification. When transmitted outside the originating organization, the document must be portion marked unless otherwise explicitly provided in the waiver approval.

d. *Additional Markings.* See Chapter III, Section, paragraph 19 (Limits to Classification and Reclassification), 20 (Reclassification After FOIA Request Receipt) and 25 (Foreign Government Information).

3. Identifying the **Original** Classification Authority, Reason for Classification, and Declassification Instruction

On hard-copy paper documents the original classification, reason and declassification instructions generally appear at the bottom, right-hand corner of the document. On cables and messages in electronic formats the marking appears in the introductory text. More detailed information is given below.

a. *Identity of Classification Authority.* The name of the Original Classification Authority (OCA) and his or her position title shall appear on the first page of each classified document on the "Classified by" line. See Treasury Order (TO) 105-19 for a list of OCA officials by position. An example of the "Classified by" line marking is as follows:

Classified by: Alexander Hamilton, Secretary of the Treasury

b. *Office of Origin.* If not otherwise evident, the DO/bureau office of origin shall be identified and follow the OCA's name on the "Classified by" line. The office of origin may either be abbreviated or spelled out. An example is:

Classified by: Andrea Donovan, Assistant Director of Security
Bureau of the Public Debt

c. *Reason for Classification.* On the "Reason" line, OCAs shall identify the rationale for classifying the information that best describes the rationale for classification to be identified as by the number 1.4 plus the corresponding letter categories, i.e., (a through h) from EO 13526 that applies. Within DO/bureaus, the following categories are the most frequently used: 1.4(b) foreign government information, 1.4(c) intelligence activities including covert action, intelligence sources or methods or cryptology, 1.4(d) foreign relations or foreign activities of the United States, including confidential sources, 1.4(e) scientific, technological, or economic matters relating to the national security, and 1.4(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security. OCAs also have the option of entering a narrative description on the "Reason" line. An example emphasizing the reason for classification is:

Classified by: Norman Carrie, Assistant Chief of Security
Internal Revenue Service
Reason: Vulnerabilities or capabilities of plans relating to the
national security; or
Reason: 1.4(g)

d. *Declassification Instructions.* At the time or original classification, the OCA shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date/event, the information shall be automatically declassified. If the OCA cannot determine an earlier specific date /event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the OCA otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision. No information may remain classified indefinitely.

The duration of the original classification decision shall be indicated on the "Declassify on" line by date or event. When a date is used it shall by identified in the following (year/month/day) format: YYYYMMDD. Events must be reasonably definite and foreseeable. Examples emphasizing the declassification instructions are shown below.

(1) A date or event for declassification corresponding to the lapse of sensitivity (less than 10 years from the date of the original decision) as in:

Classified by: Camellia Smith, Chief of Security
Financial Management Service
Reason: 1.4(g)
Declassify on: 20150110 by YYYYMMDD to indicate
January 10, 2015; or
Declassify on: Completion of Security Survey

(2) . When a specific date/event within 10 years cannot be established, the OCA shall apply the date that is exactly 10 years from the date of the original decision. On a document containing information classified on January 14, 2010, the "Declassify on" line shall appear as:

Classified by: Freda Jackson, Director of Security
Bureau of Engraving and Printing
Reason: 1.4(b)
Declassify on: 20200114 by YYYYMMDD to indicate
January 14, 2020

(3) The declassification date at 25 years of age of a document classified on October 1, 2010 would appear as follows:

Classified by: Maurice Dunkelberger, Office of Security Programs
Departmental Offices
Reason: 1.4(d)
Declassify on: 20351001 by YYYYMMDD to indicate
October 1, 2035

If the classified information should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, no date or event is required and the marking "50X1-HUM" shall be used in the "Declassify on" line.

If the classified information should clearly and demonstrably be expected to reveal key design concepts of weapons of mass destruction, no date or event is required and the marking "50X-2WMD" shall be used in the "Declassify on" line.

Classified computer media such as USB sticks, thumb/flash drives, hard drives, CD ROMs and diskettes shall be marked to indicate the highest overall classification of the information contained within the media.

4. Identifying the **Derivative** Classifier, Source(s), and Declassification Date/Event

Derivative classifiers shall carry forward instructions on the "Declassify on" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide. When a document is classified derivatively on the basis of more than one source or more than one element from a classification guide, the "Declassify on" line shall reflect the longest duration of any of its sources.

a. *Identity of Persons Applying Derivative Classification Markings.* DO/bureau documents are required to identify the derivative classifier by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified by" line.

b. *Source of Derivative Classification.* The identification of the source(s) and date(s) of the source(s) listed on the "Derived from" line, including the agency and, where available, the office of origin, and the date of the source or guide used. The reason for classification for the original decision (as reflected in the source document(s) or security classification guide), is NOT transferred in a derivative classification action. "Derived from" source dates may be spelled out or indicated by YYYYMMDD. Two examples of declassification dates at 10 and 15 years, respectively are:

(1) Classified by: Nelson Briscoe, Office of Security
Bureau of Engraving and Printing
Derived from: BEP Security Classification Guide 2,
dated January 10, 2010
Declassify on: January 10, 2020

(2) Classified by: Lisa Bloxdorf, Security Directorate
Financial Crimes Enforcement Network
Derived from: State Dept Finance Paper,
dated September 20, 2010
Declassify on: September 20, 2025

c. *Using more than One Source.* When a document is classified derivatively on the basis of more than one source document or security classification guide, the "Derived from" line shall show the phrase "Multiple Sources". The declassification date shall be the furthest future date from among the various sources used. Additionally, the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document. An example instruction is:

Classified by: Miguel Uebel, Security Manager
Bureau of Engraving and Printing
Derived from: Multiple Sources (include list thereof)
Declassify on: Date from source furthest into the future

A document derivatively classified on the basis of a source that is itself marked "Multiple Sources" shall cite the source document on its "Derived from" line rather than the term "Multiple Sources" as follows:

Classified by: Stacie Arthur, Security Chief
Internal Revenue Service
Derived from: Treasury Report entitled, "New Finance,"
dated October 20, 2010
Declassify on: October 20, 2020

d. When a document is either derivatively classified based on a source document containing the (outmoded) declassification abbreviation marking "OADR" for "Originating Agency's Determination Required", or "MR" for "Manual Review" or is from a source containing (obsolete) markings X1, X2, X3, X4, X5, X6, X7, or X8, the derivative classifier shall calculate a date that is 25 years from the date of the source document when determining a derivative document's date or event to be placed in the "Declassify on" line. Examples follow:

Derived by: Timothy Sunshine, Security Office
Office of Inspector General
Derived from: State Department cable, dated 10/20/95, Source marked OADR
Declassify on: (calculated date 10/20/20) written as 20201020

Derived by: Bob Van Deutsch, Security Division
Treasury IG for Tax Administration
Derived from: FBI letter: Tax Investigations, dated 9/2/03, Source marked X7
Declassify on: (calculated date 9/2/28) written as 20280902

e. If the source document is missing the declassification instruction, then a calculated date of 25 years from the date of the source or the current date (if the source document date is not available) shall be applied by the derivative classifier.

f. If a document is marked with the declassification instructions "DCI Only" or "DNI Only" and does not contain information described in E.O 12951, "Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems," the derivative classifier shall calculate a date that is 25 years from the date of the source document when determining a derivative document's date or event to be placed in the "Declassify on" line. If a document is marked with "DCI Only" or "DNI Only" and the information is subject to E.O. 12951, the derivative classifier shall use a date or event as prescribed by the Director of National Intelligence.

5. Unique Markings on Intelligence and Related Documents

DO/bureaus shall follow the classification marking system prescribed for the Intelligence Community (IC) when generating intelligence and related

documentation. This system uses a uniform list of security classification and control markings authorized for all dissemination of classified national intelligence information by components of the IC. This marking system augments and further defines the markings requirements established in EO 13526 for portion markings and overall classification but does not stipulate or modify the classification authority information required by EO 13526. This authorized classification and control markings register is maintained by the Controlled Access Program Coordination Office (CAPCO) also known as the CAPCO Register of the Director of National Intelligence Special Security Center. The CAPCO Register identifies the official classification and control markings, and their authorized abbreviations and portion markings. It provides for the allowable vocabulary for all national intelligence markings and other non-IC markings to control the flow of information. The CAPCO Register provides a list of the human-readable syntax for these markings, regardless of medium (e.g., text, image, graphics, electronic documents including web page, etc.).

6. Cables, Message Traffic and Electronic (E-mail) Documents

a. Markings on classified information in cables, message traffic and maintained in electronic format such as e-mail, shall conform to the same requirements, overall classification, subject lines, paragraphs/portions, "Classified by", "Derived from", "Reason", "Derived from", "Declassify on", for hard-copy paper documents. DO/bureau information systems used for classified processing might prompt the user to input specific categories of information but if system prompts do not otherwise identify these additional markings, the information shall appear in the body of the text. Derivative classifiers must be diligent to retain the designated declassification date on classified information received electronically to ensure it remains constant on email message-string traffic.

b. Whenever the markings cannot be affixed to specific classified information or materials (either hard-copy or electronic format) classifiers shall provide holders or recipients with written instructions for protecting the information. Markings shall be uniformly and conspicuously applied, leaving no doubt about the classified status of the information, the level of protection required, and the duration of classification. Electronic output must bear proper classification markings to alert users of the information to its classified status.

c. Electronic documents shall maintain traceability of classification decisions to the original classification authority. In cases where classified information in an electronic environment cannot be marked in accordance with derivative classification procedures (subject line, overall marking, paragraph/portion markings, etc.) , a warning shall be applied to alert users that the information may not be used as a source for derivative classification and providing a point of contact and instructions for users to receive further guidance on the use and classification of the information. Such information is otherwise prohibited from use as a source if it is dynamic in nature, e.g., wikis and blogs, and where

information is not marked in accordance with E.O. 13526.

d. When users modify existing electronic entries which alter the classification level of the content or add new content, they shall change the required markings to reflect the classification markings for the resulting information. Additionally, when files are attached to another electronic message or document, the overall classification of the message or document shall account for the classification level of the attachment and the message or document shall be marked

7. Declassification Extensions Up to 25 Years

An OCA may extend the duration of classification for up to 25 years from the date of the information's original classification. When the declassification date is extended, the "Declassify on" line shall be revised to include the new declassification instructions, the identity of the official authorizing the extension, and the date of this action. The official shall also make reasonable attempts to notify all holders of the information of the change in duration of classification. Classification guides applicable to such categories of information shall also be updated to reflect such revisions. An example of an extended duration of classification follows.

Classified by: Andrea Donovan, Security Division
Tax and Trade Bureau
Reason: 1.4(d)
Declassify on: Classification extended to 12/5/24 or
20241205 as in (YYYYMMDD)

8. Transmittal Documents

Transmittal documents shall indicate on the top and bottom the highest classification level of any classified information attached or enclosed. The transmittal shall also include conspicuously on its face (on the bottom, left hand side) the following statement for letters, memoranda, and email (within the text) respectively:

Letters – "Unclassified When Classified Enclosure Removed".

Memoranda and email – "Upon Removal of Attachments, this Document is (indicate classification level).

9. Foreign Government Information

Unless otherwise evident, documents that contain foreign government information (FGI) should include the marking, "This Document Contains (indicate country of origin) Information". Portions of documents containing foreign government

information shall be marked to indicate the foreign government and classification level using country codes from Chapter III, Section 8. For example, FGI from Germany would appear as "(DEU – C)" for information classified Confidential.

If the identity of the specific foreign government must be concealed, the document shall be marked, "This Document Contains Foreign Government Information" and pertinent portions shall be marked "(FGI – C)". A separate record identifying the foreign government shall be maintained in order to facilitate subsequent declassification actions.

If the fact that the information is foreign government information must itself be concealed, the markings described above shall not be used and the document shall be marked as if it were wholly of U.S. origin.

Whenever classified records are transferred for storage or for archival purposes to the National Archives and Records Administration (including temporary storage in a Federal Records Center, for example, Suitland, Maryland, the accompanying documentation shall, at a minimum, identify the boxes that contain foreign government information.

10. Working Papers

Working papers are designed as documents or material, regardless of the media, which are expected to be revised and/or collaborated until the finalized version is completed, disseminated and filed. Working papers containing classified information shall be dated when created, marked with the highest classification of any information contained therein, protected at that level, and if otherwise appropriate, destroyed when no longer needed. Whenever any of the conditions below applies, working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level.

a. Released by the originator outside of the Departmental Offices or originating Treasury bureau;

b. Retained more than 180 days from the date of origin; or

c. Filed permanently.

For accountability purposes in annually completing Standard Form 311, Agency Security Classification Program Data, only finalized documents shall be counted in reporting the volume of classified information reported. Despite multiple collaborative efforts crossing lines of authority, where working papers are finalized, the DO component or bureau of record shall be the activity to report the statistical volume of such documents or material on the SF 311.

11. Unmarked and Bulky Materials

Non-DO/bureau information contained in unmarked records, or presidential or related materials pertaining to the national defense and foreign relations of the United States, that was created 25 years ago, maintained, and protected as classified information under prior orders shall continue to be treated as classified information under E.O. 13526, and is subject to its provisions regarding declassification. With few exceptions, all DO/bureau classified information is automatically declassified at 25 years of age; see Chapter III, Section 9 with respect to downgrading and declassification.

Unmarked material reviewed and/or withdrawn from storage in the conduct of research, search/review request action or other type of examination, that is determined to contain classified information shall be marked to comply with E.O. 13526 before being returned to storage.

Bulky material, equipment, and facilities, etc., shall be clearly identified in a manner that leaves no doubt about the classification status of the material, the level of protection required, and the duration of classification. Upon a finding that identification would itself reveal classified information, such identification is not required. Supporting documentation for such a finding must be maintained in the appropriate security facility.

12. Classification by Compilation/Aggregation

A compilation of items that are individually unclassified may be classified if the aggregated information meets the standards established by the E.O. and reveals an additional association or relationship, as determined by the original classification authority. Any unclassified portions shall be portion marked (U), while the overall markings shall reflect the classification of the compiled information even if all portions are marked unclassified. In any such situation, clear instructions must appear with the aggregated information explaining the unique circumstances under which the individual portions constitute a classified compilation, and when they do not.

Chapter III **Foreign Classification Markings** Updated
Section 7 8/28/14

1. Introduction

Classified information provided by a foreign government requires the equivalent level of protection to that required by the foreign government or international organization of governments furnishing the information to the United States. Departmental Offices (DO) and bureau users are required to protect foreign government information to the extent adequate to achieve equivalency with U.S. classified information.

2. Foreign Equivalent Markings

Foreign government information may either retain its own (foreign) classification marking or be assigned an equivalent U.S. classification marking. Most countries use a three-tier system similar to the United States (Top Secret, Secret, and Confidential). Some countries, however, rely on a two- or even a four-tier system for identifying their classified information.

The following chart shows the equivalent classification markings used by particular countries to properly identify their classified information. It shall be used in determining the equivalent U.S. Government classification when applied to foreign government information by DO/bureaus.

3. Foreign Markings Chart

Nation	*Top Secret*	*Secret*	*Confidential*	*Restricted*
Argentina	Estrictamente Secreto	Secreto	Confidencial	Reservado
Australia	Top Secret	Secret	Confidential	Restricted
Austria	Streng Geheim	Geheim	Verschluss	- - - - - - - -
Belgium (Flemish)	Zeer Geheim	Geheim	Vertrouwelijk	Bespertke Verspreiding
Bolivia	Supersecreto or Muy Secreto	Secreto	Confidencial	Reservado
Brazil	Ultra Secreto	Secreto	Confidencial	Reservado
Britain (UK)	UK Top Secret	UK Secret	No equivalent	No equivalent
Cambodia	Sam Ngat Bamphot	Sam Ngat	Roeung Art Kambang	Ham Kom Psay
Canada	Top Secret	Secret	Confidential	Restricted
Chile	Secreto	Secreto	Reservado	Reservado
Columbia	Untrasecreto	Secreto	Reservado	Confidencial Restringido
Costa Rica	Alto Secreto	Secreto	Confidencial	
Denmark	Yderst Hemmeligt	Hemmeligt	Fortroligt	Tiltjenestebrug

Nation	*Top Secret*	*Secret*	*Confidential*	*Restricted*
Ecuador	Secretisimo	Secreto	Confidencial	Reservado
Egypt	Jirri Lilghaxeh	Sirri	Khas	Mehoud Jidden
El Salvador	Ultra Secreto	Secreto	Confidencial	Reservado
Ethiopia	Yemiaz Birtou Mistir	Mistir	Kilkil	- - - - - - - -
Finland	Etittain Salainen	Salainen	- - - - - - - -	- - - - - - - -
France	Tres Secret	Secret Defense	Confidentiel Defense	Diffusion Restreinte
Germany	Streng Geheim	Geheim	Vs-Vertraulich	
Guatemala	Alto Secreto	Secreto	Confidencial	Reservado
Haiti	Top Secret	Secret	Confidential	Reserve
Honduras	Super Secreto	Secreto	Confidencial	Reservado
Hong Kong	Top Secret	Secret	Confidential	Restricted
Hungary	Szigoruan Titkos	Titkos	Bizalmas	- - - - - - - -
India	Param Gupt	Gupt	Gopniya	Pratibanhst / seemit
Indonesia	Sangat Rahasia	Rahasia	Agak Rahahasia	Terbatas
Iran	Bekoliserri	Serri	Kheil Mahramaneh	Mahramaneh
Iraq	Sirri Lil-ghaxah	Sirri	Khass	Mehdoud
Ireland	Algjorti	Trunadarmal	- - - - - - - -	- - - - - - - -
Ireland (Gaelic)	An-sicreideah	Sicreideach	Runda	Srianta
Israel	Sodi Beyoter	Sodi	Shamur	Mugbal
Italy	Secgretissimo	Segreto	Riservatissimo	Riservat
Japan	Kimitsu	Gokuhi	Hi	Toriatsukaichui
Jordan	Maktun Jiddan	Maktum	Sirri	Mahdud
Korea	I-Kup Bi Mil	II-Kup Bi Mil	III-Kup Bi Mil	Bu Woi Bi
Laos	Lup Sood Gnod	Kaum Lup	Kaum Lup	Chum Kut Kon Arn
Lebanon	Tres Secret	Secret	Confidentiel	- - - - - - - -
Mexico	Alto Secreto	Secreto	Confidencial	Restringido
Netherlands	Zeer Geheim	Geheim	Confidentieel or Vertrouwelijk	Dienstgeheim
New Zealand	Top Secret	Secret	Confidential	Restricted
Nicaragua	Alto Secreto	Secreto	Confidencial	Reservado
Norway	Strengt Hemmelig	Hemmelig	Konfidensiell	Begrenset
Pakistan	Intahai Khufia	Khufia	Sinha-E-Raz	Barai Mahdud Taqsim
Paraguay	Secreto	Secreto	Confidencial	Reservado
Peru	Estrictamente Secreto	Secreto	Confidencial	Reservado
Philippines	Top Secret	Secret	Confidential	Restricted
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Saudi Arabia	Saudi Top Secret	Saudi Very Secret	Saudi Secret	Saudi Restricted
South Africa (Afrikaans)	Top Secret Uiters Geheim	Secret Geheim	Confidential Vertroukik	Restricted Besperk

Nation	*Top Secret*	*Secret*	*Confidential*	*Restricted*
Spain	Maximo Secreto	Secreto	Confidencial	Diffusion Limitada
Sweden	Hemlig (double red borders)	Hemlig (single red border)	- - - - - - - -	- - - - - - - -
Switzerland	*(Three languages: French, German, and Italian. Top Secret has a registration number to distinguish it from Secret and Confidential).*			
Taiwan	Chichimi	Chimi	- - - - - - - -	- - - - - - - -
Thailand	Lup Tisud	Lup Maag	Lug	Pok Pid
Turkey	Cok Gizli	Gizl	Ozel	Hizmete Ozel
United Kingdom	UK Top Secret	UK Secret	No equivalent	No equivalent
Uruguay	Ultra Secreto	Secreto	Confidencial	Reservado
Vietnam	Toi-Mat	Mat	Kin	Pho Bien Han Che

NOTE: Greece and Russia each have 4-tiered classification systems in the Greek and Cyrillic alphabets, respectively. Chinese characters are not conducive to the above chart.

Chapter III
Section 8

Country Codes Used for Marking Classified Information

Updated
6/17/11

1. Introduction

Country codes are used to identify classified documents and materials that are pre-approved by proper U.S. Government authority for release to specific countries and to their nationals with equivalent, foreign government-issued security clearances. Individual country codes are abbreviated designations associated with particular nations. The three-letter country codes are listed in part 3.

2. Coding System

The three-letter system of country codes developed by the intelligence community (IC) shall be used by Treasury/bureaus. Country-code designations shall be used in conjunction with the terms "REL TO" (releasable or releasable to) markings and the applicable classification level. For example, if the classification level is "Secret" and the information is "releasable to" Germany, the coding is "SECRET//REL TO USA, DEU." The inclusion of release to the United States or USA is also required on all coding which is in all upper case letters. Another example is "CONFIDENTIAL//REL USA, ARG, PRY" which is "Confidential information releasable to (U.S.) and Argentina and Paraguay."

Where incoming country codes on source documents differ from the IC standard, Treasury/bureau derivative classifiers shall apply the three-letter country code in lieu of the code on the source document(s). For example, if the incoming document is marked "SECRET//REL TO USA, UK," the Treasury/bureau document shall be marked "SECRET//REL TO USA, GBR" to reflect that particular Secret information is releasable to the United Kingdom.

Foreign release authority and instructions for proper release may only be accomplished in consultation and coordination with the Special Security Office, Office of the Assistant Secretary for Intelligence and Analysis.

3. Three-letter Country Codes

As changes are made in the country code listing they will be updated on the Treasury Office of Security Programs website. The list of changes is that applied from 1989 to 2010. The three-letter country codes shall be used to identify the following countries, possessions and territories:

AFGHANISTAN	AFG
ALAND ISLANDS	ALA
ALBANIA	ALB
ALGERIA	DZA
AMERICAN SAMOA	ASM
ANDORRA	AND
ANGOLA	AGO
ANGUILLA	AIA
ANTARCTICA	ATA
ANTIGUA AND BARBUDA	ATG
ARGENTINA	ARG
ARMENIA	ARM
ARUBA	ABW
AUSTRALIA	AUS
AUSTRIA	AUT
AZERBAIJAN	AZE
BAHAMAS, THE	BHS
BAHRAIN	BHR
BANGLADESH	BGD
BARBADOS	BRB
BELARUS	BLR
BELGIUM	BEL
BELIZE	BLZ
BENIN	BEN
BERMUDA	BMU
BHUTAN	BTN
BOLIVIA, PLURINATIONAL STATE of	BOL
BOSNIA AND HERZEGOVINA	BIH
BOTSWANA	BWA
BOUVET ISLAND	BVT
BRAZIL	BRA
BRITISH INDIAN OCEAN TERRITORY	IOT
BRUNEI DARUSSALAM	BRN
BULGARIA	BGR
BURKINA FASO	BFA
BURUNDI	BDI
CAMBODIA	KHM
CAMEROON	CMR
CANADA	CAN
CAPE VERDE	CPV
CAYMAN ISLANDS	CYM
CENTRAL AFRICAN REPUBLIC	CAF
CHAD	TCD
CHILE	CHL

CHINA, PEOPLE'S REPUBLIC of..... CHN
CHRISTMAS ISLAND ..... CXR
COCOS (KEELING) ISLANDS ..... CCK
COLUMBIA ..... COL
COMOROS ..... COM
CONGO, DEMORATIC REPUBLIC of..... COD
CONGO, REPUBLIC of the ..... COG
COOK ISLANDS ..... COK
COSTA RICA..... CRT

COTE D'IVOIRE CIV
CROATIA (local name HRVATSKA) ..... HRV
CUBA..... CUB
CYPRUS ..... CYP
CZECH REPUBLIC ..... CZE

DENMARK..... DNK
DJIBOUTI..... DJI
DOMINICA..... DMA
DOMINICAN REPUBLIC..... DOM

ECUADOR..... ECU
EGYPT..... EGY
EL SALVADOR..... SLV
EQUATORIAL GUINEA ..... GNQ
ERITREA ..... ERI
ESTONIA..... EST
ETHIOPIA..... ETH

FALKLAND ISLANDS (MALVINAS)..... FLK
FAROE ISLANDS..... FRO
FIJI..... FJI
FINLAND ..... FIN
FRANCE ..... FRA
FRANCE, METROPOLITAN.....FXX
FRENCH GUIANA ..... GUF
FRENCH POLYNESIA .. .. PYF
FRENCH SOUTHERN TERRITORIES..... ATF

GABON..... GAB
GAMBIA..... GMB
GAZA STRIP see PALESTINE TERRITORY,
OCCUPIED.....
GEORGIA ..... GEO
GERMANY ..... DEU

GHANA ..... GHA
GIBRALTAR ..... GIB
GREECE ..... GRC
GREENLAND ..... GRL
GRENADA ..... GRD
GUADELOUPE ..... GLP
GUAM ..... GUM
GUATEMALA ..... GTM
GUERNSEY ..... GGY
GUINEA ..... GIN
GUINEA-BISSAU ..... GNB
GUYANA ..... GUY

HAITI ..... HTI
HEARD ISLAND and MCDONALD ISLANDS ..... HMD
HOLY SEE (VATICAN CITY STATE) ..... VAT
HONDURAS ..... HND
HONG KONG ..... HKG
HUNGARY ..... HUN

ICELAND ..... ISL
INDIA ..... IND
INDONESIA ..... IDN
IRAN, ISLAMIC REPUBLIC of ..... IRN
IRAQ ..... IRQ
IRELAND ..... IRL
ISLE OF MAN ..... IMN
ISRAEL ..... ISR
ITALY ..... ITA

JAMAICA ..... JAM
JAPAN ..... JPN
JERSEY ..... JEY
JORDAN ..... JOR

KAZAKHSTAN ..... KAZ
KENYA ..... KEN
KIRIBATI ..... KIR
KOREA, DEMOCRATIC PEOPLE'S REPUBLIC of ..... PRK
KOREA, REPUBLIC of (SOUTH) ..... KOR
KUWAIT ..... KWT
KYRGYSTAN ..... KGZ

LAO PEOPLE'S DEMOCRATIC REPUBLIC (LAOS) ... LAO
LATVIA ..... LVA
LEBANON ..... LBN

LESOTHO ..... LSO
LIBERIA ..... LBR
LIBYAN ARAB JAMAHIRIYA (LIBYA) ..... LBY
LIECHTENSTEIN ..... LIE
LITHUANIA ..... LTU
LUXEMBOURG ..... LUX

MACAO ..... MAC
MACEDONIA (FORMER YUGOSLAV REPUBLIC of). MKD
MADAGASCAR ..... MDG
MALAWI ..... MWI
MALAYSIA ..... MYS
MALDIVES ..... MDV
MALI ..... MLI
MALTA ..... MLT
MARSHALL ISLANDS ..... MHL
MARTINIQUE ..... MTQ
MAURITANIA ..... MRT
MAURITIUS ..... MUS
MAYOTTE ..... MYT
MEXICO ..... MEX
MICRONESIA, FEDERATED STATES of ..... FSM
MOLDOVA, REPUBLIC of ..... MDA
MONACO ..... MCO
MONGOLIA ..... MNG
MONTENEGRO ..... MNE
MONTSERRAT ..... MSR
MOROCCO ..... MAR
MOZAMB IQUE ..... MOZ
MYANMAR (BURMA) ..... MMR

NAMIBIA ..... NAM
NAURU ..... NRU
NEPAL ..... NPL
NETHERLANDS ..... NLD
NETHERLANDS ANTILLES ..... ANT
NEW CALEDONIA ..... NCL
NEW ZEALAND ..... NZL
NICARAGUA ..... NIC
NIGER ..... NER
NIGERIA ..... NGA
NIUE ..... NIU
NORFOLK ISLAND ..... NFK
NORTHERN MARIANA ISLANDS ..... MNP
NORWAY ..... NOR

OMAN ..... OMN

PAKISTAN ..... PAK
PALAU ..... PLW
PALESTINIAN TERRITORY, OCCUPIED
(GAZA STRIP) ..... PSE
PANAMA ..... PAN
PAPUA NEW GUINEA ..... PNG
PARAGUAY ..... PRY
PERU ..... PER
PHILIPPINES ..... PHL
PITCAIRN ..... PCN
POLAND ..... POL
PORTUGAL ..... PRT
PUERTO RICO ..... PRI

QATAR ..... QAT

REUNION ..... REU
ROMANIA ..... ROU
RUSSIAN FEDERATION ..... RUS
RWANDA ..... RWA

SAHARA OCCIDENTAL (see WESTERN SAHARA) .....
SAINT BARTHELMY .....BLM
SAINT HELENA, ASCENSION and
TRISTAN da CUNHA ..... SHN
SAINT KITTS and NEVIS ..... KNA
SAINT LUCIA ..... LCA
SAINT MARTIN (FRENCH PART) .....MAF
SAINT PIERRE and MIQUELON ..... SPM
SAINT VINCENT and the GRENADINES ..... VCT
SAMOA ..... WSM
SAN MARINO .....SMR
SAO TOME and PRINCIPE ..... STP
SAUDI ARABIA ..... SAU
SENEGAL ..... SEN
SERBIA ..... SCG
SEYCHELLES ..... SYG
SIERRA LEONE ..... SLE
SINGAPORE ..... SGP
SLOVAKIA (SLOVAK REPUBLIC) ..... SVK
SLOVENIA ..... SVN
SOLOMON ISLANDS ..... SLB
SOMALIA ..... SOM
SOUTH AFRICA ..... ZAF

SOUTH GEORGIA and the SOUTH SANDWICH ISLANDS ..... SGS
SPAIN ..... ESP
SRI LANKA ..... LKA
SUDAN ..... SDN
SURINAME ..... SUR
SVALBARD and JAN MAYEN ..... SJM
SWAZILAND ..... SWZ
SWEDEN ..... SWE
SWITZERLAND ..... CHE
SYRIAN ARAB REPUBLIC ..... SYR

TAIWAN, PROVINCE of CHINA ..... TWN
TAJIKISTAN ..... TJK
TANZANIA, UNITED REPUBLIC of ..... TZA
THAILAND ..... THA
TIMOR-LESTE ..... TLS
TOGO ..... TGO
TOKELAU ..... TKL
TONGA ..... TON
TRINIDAD and TOBAGO ..... TTO
TUNISIA ..... TUN
TURKEY ..... TUR
TURKMENISTAN ..... TKM
TURKS and CAICOS ISLANDS ..... TCA
TUVALU ..... TUV

UGANDA ..... UGA
UKRAINE ..... UKR
UNITED ARAB EMIRATES ..... ARE
UNITED KINGDOM ..... GBR
UNITED STATES ..... USA
UNITED STATES MINOR OUTLYING ISLANDS ..... UMI
URUGUAY ..... URY
UZBEKISTAN ..... UZB

VANUATU ..... VUT
VENEZUELA, BOLIVARIAN REPUBLIC of ..... VEN
VIET NAM ..... VNM
VIRGIN ISLANDS (BRITISH) ..... VGB
VIRGIN ISLANDS (US) ..... VIR

WALLIS and FUTUNA ISLANDS ..... WLF

WEST BANK (see PALESTINIAN TERRITORY) .....

WESTERN SAHARA (SAHARA OCCIDENTAL).....ESH

YEMEN..... YEM

ZAMBIA ..... ZMB
ZIMBABWE..... ZWE

Chapter III **Downgrading and Declassification** Updated
Section 9 6/17/11

1. Downgrading

Downgrading is the determination by a downgrading/declassification authority, that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level, e.g., from Top Secret to Secret or from Secret to Confidential and applying appropriate markings on such documents to reflect this change in status, the identity of the downgrading/declassification official and notification to authorized recipients of the reduced status.

2. Declassification

Declassification is the authorized change in the status of information from classified to unclassified information. It includes applying appropriate markings on such documents to reflect this reduced status, the identity of the declassification official and notification to authorized recipients of the change in status. The basic premise is information shall be declassified as soon as it no longer meets the standards for continued classification under Executive Order (E.O.) 13526, and with due respect to protecting foreign government information as well as foreign confidential sources.

In some cases the need to protect classified information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the Secretary of the Treasury or the Department's Senior Agency Official (SAO), via Treasury's Director, Office of Security Programs (OSP). Either official will determine, at their discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural rights subject to judicial review.

3. Downgrading and Declassification Authority

Downgrading and declassification may be exercised by the Departmental Offices (DO) or bureau official authorizing the original classification (if the official is still serving in the same position); a successor; a supervisory official; or, an official delegated original classification authority by the Secretary of the Treasury or the Department's SAO; the DAS for Security as identified in Treasury Order (TO) 105-19, *Delegation of Original Classification Authority; Requirements for Declassification and Downgrading,*

DO/bureau officials identified in TO 105-19 may automatically downgrade and declassify information within their jurisdiction up to the level of their own security

clearance. Where the official does not have the same level of original classification authority as the document(s) subject to review, the decision shall be referred to the next higher level official for formal approval. Referrals shall include recommendations as to continued classification, downgrading, or declassification, whether in full or in part.

The Secretary may delegate downgrading and declassification at the Top Secret, Secret, and Confidential levels. The SAO may delegate downgrading and declassification at the Secret and Confidential levels. All such delegations to officials not otherwise identified in TO 105-19 shall be updated annually (in coordination with the Director, OSP), and in writing on Treasury Department Form (TD F) 15-05.3, *Report of Authorized Downgrading and Declassification Officials*. Officials so identified may not downgrade or declassify information that exceeds the level of their own security clearance. Whenever the SAO position is vacant, the Deputy Assistant Secretary for Security will automatically serve as the Acting SAO and exercise the full authority of the SAO on information security matters. If both positions are vacant, the Director, OSP will serve as the Acting SAO.

Downgrading and declassification authority may only be applied to Treasury/bureau originated information. Treasury/bureau reviewers may provide recommendations from a Departmental perspective, but any decision to downgrade or declassify another agency's classified information must be deferred to the originating agency or department.

4. Unofficial Publication or Disclosure

Following an inadvertent or unauthorized disclosure or publication of information identical or similar to information that has been classified in accordance with EO 13526 or predecessor Orders, a determination shall be made of the degree of damage to the national security, the need for continued classification, and, in coordination with the DO/bureau organization or outside agency in which the disclosure occurred, what action(s) must be taken to prevent similar occurrences. Classified information shall not be automatically declassified as a result of an unauthorized disclosure as for example, in the news media. Prior to public release, all declassified records shall be appropriately marked to reflect the declassified status of the information.

5. Downgrading and Declassification Markings

Whenever a change is made in the original classification to downgrade classified information, it shall be promptly and conspicuously marked to indicate the reduced status. If declassification markings cannot be affixed to specific information or materials, holders or recipients of the information shall be provided with written instructions for marking the information. Markings shall be uniformly and conspicuously applied to leave no doubt about the declassified status of the information and who authorized the declassification. The following markings shall be applied to records, or copies of records, regardless of media:

a. The word, "Declassified" or term "Declassified by the Treasury Department or Bureau Name".

b. The identity of the declassification authority by name and position, or by personal identifier, or the title and date of the declassification guide.

c. The date of the declassification action.

Earlier classification markings shall be lined out with either an "X" or straight line, cancelled or otherwise obliterated (in part or full at the discretion of the authorized downgrading and declassification official) including individual pages and paragraphs/portions throughout the document.

Information in bulk records storage shall be labeled on the exterior of the security container or bar-lock cabinet (until October 1, 2012) to alleviate the burden of re-marking significant record holdings. However, individual documents withdrawn from storage for review and/or further dissemination shall be marked to reflect the downgraded or declassified status.

Information officially declassified by DO/bureaus shall be marked to leave no doubt about its declassified status. The fact that particular newly-declassified information of DO/bureau origin was previously classified at a given level is not a sensitivity concern. It should normally not matter with respect to determining whether the now-declassified information can be released. However, declassification itself does not mean the information is automatically releasable; there might be particular reasons for withholding information from release as for example under the Freedom of Information and Privacy Acts. If in doubt, consult with DO/bureau subject matter experts, security officials and/or records management officials for guidance. In the case of SCI information that has been declassified, guidance shall be obtained from the Office of the Assistant Secretary for Intelligence and Analysis.

6. Classified Documents Requested by Departing Officials

Treasury Order (TO) 25-05, *The Freedom of Information Act,* and TO 80-05, *Records and Information Management Program,* contain procedural steps for ensuring current DO/bureau employees, departing employees, consultants, and contractor personnel do not remove documentary materials from DO/bureau custody without written authorization. Classified documents may not be removed by departing DO/bureau officials unless and until the information has been officially reviewed, declassified, marked accordingly, and approved for removal under the above TOs.

The standard for any declassification actions shall be the degree to which existing classified information no longer warrants continued protection in the national security interest. Prior to any decision being made, documents shall be reviewed by properly cleared subject-matter experts for their opinion and formal judgment. Declassification

decisions must be made by either the originator/successor or by an authorized downgrading/declassification official. Final decisions shall be rendered on a document-by-document basis.

The fact that departing political appointees or career officials may prefer to take such information with them or may request that it be declassified and released to them will not be a consideration in the declassification of official DO/bureau classified records or file series. The national security needs to safeguard classified information supersede the personal preferences of departing officials. Such departing officials shall not declassify information or instruct subordinates to declassify information that they request for removal, or under any circumstance remove classified documents or material originated by another agency or department that had been provided to DO/bureaus; by a foreign government; from an international organization of governments; or any elements thereof. Non-Treasury originated classified information must be referred to the originating Federal agency or department, or the foreign originators, for decision, as appropriate.

7. Transferred Classified Records

In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving DO/bureau entity shall be deemed to be the originating agency.

Classified records originating in a DO/bureau entity that has ceased to exist and for which there is no successor shall be deemed to be the responsibility of the current holder. Such records may be declassified or downgraded by those in possession after consultation with any other agency that has an interest in the subject-matter of the records. Classified records accessioned into the National Archives and Records Administration (National Archives) as of the effective date of E.O. 13526 shall be declassified or downgraded by the Archivist of the United States in accordance with the Order, directives issued pursuant to the Order, DO/bureau declassification guides, and any existing procedural agreement between the Archivist and the Secretary of the Treasury.

DO/bureau records management officials and those offices responsible for originally classifying information shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before the records are accessioned into the National Archives. The Archivist may also require that classified records be accessioned into the National Archives when necessary to comply with provisions of the Federal Records Act. This provision does not apply to records being transferred to the Archivist pursuant to Section 2203 (44 USC) or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

10. Mandatory Review for Declassification

Mandatory review is a mechanism through which the public can request declassification review of classified records, regardless of age or origin, subject to certain limitations set forth EO 13526, i.e., the request describes the document or material containing the information in sufficient specificity to enable DO/bureaus to locate it with a reasonable amount of effort; the document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. 552 in accordance with law; and the information is not the subject of pending litigation.

Where particular information is determined to no longer meet the standards for classification under EO 13526, the information shall be declassified and released unless withholding is otherwise authorized and warranted under applicable law. If DO/bureaus have previously reviewed particular information for possible declassification within the last 2 years, they need not conduct another review. Accordingly the requester shall be so informed of this fact and the prior review decision along with advising the request of appeal rights.

Treasury's procedures for requesting and processing mandatory declassification reviews of classified information are contained in 31 CFR Part 2, *National Security Information*, and published in the Federal Register

Requests for mandatory declassification reviews are not limited to U.S. citizens, permanent resident aliens, Federal agencies, or a state or local government. Except as provided by Section 3.5(b), E.O. 13526 all information classified by DO/bureaus under this Order or any predecessor Order shall be subject to mandatory declassification review. When conducting mandatory declassification reviews the information shall be declassified if it no longer meets the classification standards. DO/bureaus receiving mandatory review requests are expected to conduct a line-by-line review of the record(s) for public access and are expected to release the information to the requestor, unless that information is prohibited from release under the provisions of a statutory authority, such as, but not limited to, the Freedom of Information Act (5 U.S.C., 552), a amended, the Presidential Records Act of 1978 (44 U.S.C. 2201-2207), or the National Security Act of 1947 (Public Law 235, 61 Stat. 496, 50 U.S.C. Chapter 15). The following conditions apply to mandatory review.

a. Each request must describe the document or material containing the information with sufficient specificity to enable the DO/bureau to locate it in their file holdings with a reasonable amount of effort. Declassification review requests that are forwarded by a Presidential Library or other U.S. Government agency (with that agency's recommendations about declassification and release) are normally accompanied by the classified documents and should not require records search. Requests for broad types of information, entire file series of records, or similar non-specific requests may be denied for processing. Additionally, if the information has been reviewed by a DO/bureau within the past two years, or the information is the subject of pending litigation, the DO/bureau shall inform the requester of this fact and appeal rights.

b. In responding to mandatory declassification review requests, DO/bureaus shall make a final determination within one year from the date of receipt. When information cannot be declassified in its entirety, reasonable efforts shall be made to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Upon denial, in whole or in part, of an initial request, the requestor shall be notified of the right of an administrative appeal which must be filed within 60 days of receipt of the denial.

c. *Requests for Classified Records in the Custody of a Non-Treasury Agency.* When DO/bureaus receive a mandatory declassification review request for records in their possession that were originated by a non-Treasury agency, it shall refer the request and the pertinent records to that agency. DO/bureaus shall provide written notice to the originating agency of their opinion with respect to possible declassification and/or release to enable DO/bureau views to be taken into consideration.

d. *Fees for Mandatory Review.* Fees for mandatory review may be imposed by the Treasury/bureaus for significantly voluminous and bulky requests involving search and/or review time.

(1) For searches that take more than two hours or for review times that takes greater than two hours, the rate of a GS-11 Step 1 employee, in the Washington-Baltimore Federal pay area, in effect when the request is received by the Office of Security Programs (OSP), shall apply. The first 100 pages of fully or partially releasable documents are free. The cost of additional pages is 20 cents per page. This same fee schedule shall apply to other instances where services of DO/bureau employees are rendered for search and review of records, as warranted.

(2) Collection of fees may be waived, in writing, by a bureau head or the equivalent DO/bureau official at the Assistant Secretary or equivalent level. Fees are payable by check or money order to the Treasurer of the United States.

9. Processing Mandatory Declassification Review Requests

Requests for mandatory declassification review shall normally be addressed to the Assistant Director (Information Security), Office of Security Programs, 1500 Pennsylvania Avenue, NW, Washington, DC 20220. Treasury bureaus directly receiving a mandatory declassification review request from outside the Department shall process the request and report statistical information related thereto in their annual submission of Standard Form 311, (Agency Security Classification Program Management Data). If a

request does not reasonably describe the information sought, OSP will notify the requester that unless additional information is provided or the scope of the request is narrowed, no further action will be taken.

When OSP receives a mandatory declassification review request it will determine the appropriate DO office(s) and/or bureau(s) that should: (1) review the documentation; or, (2) conduct a search of their pertinent file records in tasking the affected DO/bureau office(s). In referring classified information, the OSP will:

a. Identify the originator of the request (if other than DO/bureau origin).

b. Describe the document(s) or material.

c. Assign a target date for completion of the review.

d. Provide technical advice with respect to inquiries concerning such mandatory declassification review requests (including actions required by DO/bureaus).

The OSP will ensure required markings are applied to outgoing copies of the reviewed document(s) or material in conformance with E.O. 13526. When completed, the OSP will respond on behalf of the DO/bureaus and close out each mandatory declassification review request with the affected Presidential Library and/or other Federal agency. This includes notifying requesters of their right to administratively appeal any decisions-to-deny or to not fully declassify information for which DO/bureaus are responsible.

a. *Process for DO/Bureau Security Officers/Points of Contact to Use.* When an appeal is made, the DO/bureau security officer or security contact will take the following steps:

(1) Acknowledge receipt and safeguard classified document(s) or material contained in mandatory declassification review requests forwarded to them by the OSP.

(2) Determine and assign responsibility for each referred request within their DO/bureau office to those cleared people with subject-matter knowledge and/or interest based on established need-to-know criteria for classified information, and track the internal review process. Reviewing officials shall make a final determination within 60 calendar days of receipt. However, if materials subject to review are overly voluminous and bulky, additional review time may be authorized provided such a request is made in writing along with a target date for completion. All DO/bureau requests for additional review time must be in writing and sent to the Assistant Director (Information Security), OSP for determination.

(3) Retrieve, and as needed, conduct a search of records previously forwarded to Federal records storage or still housed within current and/or active files.

This includes identifying the need for any document(s) to be reviewed by other DO/bureau components or Federal agencies.

(4) Reporting the amount of search or review time is no longer required except where fees are being imposed for requests involving a significant bulk volume of records. Where fees are being charged, DO/bureaus shall assist in determining the search and/or review time. OSP in coordination with records management officials may request pre-payment where the cost is likely to exceed $500 and in ensuring the requester's written agreement to underwrite the cost.

(5) Process mandatory declassification reviews in a timely manner and follow-up with the OSP upon finalization. The written response must identify the following information:

- Any section(s) of the document(s) requiring continued classification, with corresponding paragraph/portion markings (including subjects and titles), if not already affixed to the document(s).
- The rationale for continued classification under E.O. 13526, as applicable, or exception to release as identified in paragraph 7 above.
- The new date/event for declassification or any objection(s) to declassification and release.
- When the DO/bureau decision is that the document(s) can be declassified in full, the response shall so indicate.

(6) Apply required markings on file copies of reviewed material retained that reflect the decision with respect to declassification and release. The same DO/bureau reviewer(s) shall notify known DO/bureau and non-Treasury holders of records of their determination(s).

10. Appeals of Declassification Decision Denials

If a decision by DO/bureau reviewers to not fully declassify documents or material that are subject to a mandatory declassification review is appealed, a new decision shall be rendered. Such appeals must be filed within 60 calendar days of receipt of the denial. If additional time is required to make a determination the requestor shall be so notified and provide the requestor with the reason for the extension. The appellate review and evaluation of the document(s) or material shall be conducted by appropriately cleared DO/bureau employees with jurisdictional authority over the information and be completed within 30 calendar days. If more time is required, the appellate authority shall

notify the requester and state the reason(s). Appellate reviewers may rely on the recommendation(s) of the previous reviewer(s) to sustain or overrule the initial decision. The appellate authority shall be at a higher level if a Deputy Assistant Secretary or equivalent official was the initial decision-maker. The appellate authority shall inform the requestor of their final appeal rights to the Interagency Security Classification Appeals Panel.

11. Foreign Relations of the United States Series

DO/bureaus shall assist the Department of State (DOS) in its review and preparation of releasable material for the Foreign Relations of the United States (FRUS) series. With due regard to normal security requirements, DO/bureaus shall facilitate access to appropriate classified information in their custody and expedite the declassification review of documents proposed for inclusion in this series. Services provided to the DOS for the FRUS series shall be at no cost.

12. Requests for Documents containing Foreign Government Information

Requests for documents containing foreign government information shall be handled in the same manner as other requests within the DO/bureau that received, or derivatively classified information (containing the foreign government information) and in making the declassification determination upon consultation with affected agencies. If the information was not classified by DO/bureaus, it shall be referred to the agency that did classify it for their action, processing, and disposition. Consultation with the State Department shall determine whether the information is subject to a treaty or international agreement that does not permit automatic or unilateral declassification.

13. Requests for Cryptologic and Intelligence Information

Requests for cryptologic information shall be processed in accordance with special procedures issued by the Secretary of Defense and when cryptologic information pertains to intelligence activities under special procedures issued by the Director of National Intelligence (DNI). Mandatory declassification review requests pertaining to intelligence sources, methods, and activities shall be processed in accordance with special procedures issued by the DNI. Within DO/bureaus, the request shall be forwarded to and handled by the Office of the Assistant Secretary for Intelligence and Analysis.

14. Systematic Review for Declassification

Systematic review applies to records (including Presidential papers) originally classified by DO/bureaus, which the Archivist of the United States has determined to be of sufficient historical, or other, value to warrant permanent retention and which are exempt from automatic declassification under Section 3.4, E.O. 13526. The Archivist establishes

records priorities based on the degree of researcher interest and the likelihood of declassification following such review. To assist the Archivist in the conduct of systematic reviews, DO/bureaus shall develop declassification guides for classified information they originate in consultation with the Archivist of the United States and the Information Security Oversight Office (ISOO). Such guidelines shall be reviewed and updated at least every five years unless the Archivist requests earlier review. Non-permanent classified records shall be disposed of in accordance with schedules approved by the Administrator of General Services, General Services Administration (GSA), under the Records Disposal Act and coordinated with DO/bureau records management officials.

DO/bureaus shall follow any special procedures for systematic review of classified records pertaining to intelligence activities (including special activities), or intelligence sources or methods, or cryptology, issued by the DNI.

15. National Declassification Center

The National Declassification Center was established within the National Archives and Records Administration to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. In consultation with representative of the Center's participating (member) agencies and after input from the general public, the Archivist shall develop priorities for declassification activities that take into account the degree of researcher interest and the likelihood of declassification.

DO/bureaus may establish centralized facilities and internal operations to conduct internal declassification reviews as appropriate to achieve optimized records management and declassification business processes.

16. Automatic Declassification

All classified information contained in records that are more than 25 years old and that have been determined to have permanent historical value will be automatically declassified, unless such material has been exempted (under Title 44 U.S.C. via the ISOO) and in coordination with the Director, OSP. The 25-year automatic declassification process is a sliding scale as records age and applies annually to classified information every December 31st. The premise is that 25-year old documents can be declassified based on their age and subject matter when continued protection as national security information is no longer necessary.

The exemption ensures continued classification of only particular information warranting protection in the national interest despite the passage of time. The automatic declassification review process also includes identifying the classified equities of other agencies for appropriate referral. Responsibility for identifying other agencies classified equities in derivatively classified documents with respect to automatic declassification under Section 3.3, E.O. 13526 resides with the DO/bureau component offices that

generated such documents and records.

a. *Exemption criteria.* The Secretary of the Treasury or the SAO on that official's behalf may exempt from automatic declassification specific information, the release of which could be expected to:

- Reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method.
- Reveal information that would assist in the development or use of weapons of mass destruction.
- Reveal information that would impair U.S. cryptologic systems or activities.
- Reveal information that would impair the application of state-of-the-art technology within a U.S. weapons system.
- Reveal actual U.S. military war plans that remain in effect.
- Reveal information, including foreign government information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States.
- Reveal information that would clearly and demonstrably impair the current ability of U.S. Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized.
- Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security.
- Violate a statute, treaty, or international agreement.

b. *Declassification Guide.* DO/bureaus shall narrowly define and clearly state why particular information should be exempt and develop a guide with sufficient detail to permit reviewers to readily understand what specific information is exempted from automatic declassification. The guide shall do the following:

- Identify the subject matter, the original declassification authority, the date of issuance or last review, and shall state precisely the elements or

categories of information to be declassified, to be downgraded, or not to be declassified.

- Cite a clear relationship to specific exemptions and, if necessary, explain how the information fits in the category or categories cited, and then provide a reasonable explanation or justification for the exemption.

- Include a fixed date for future declassification.

c. *Exemptions*. Exemptions from automatic declassification are intended for records that, during DO/bureau reviews, are determined to require further classification beyond the 25-year mark. Exemptions from automatic declassification are not valid until approved by the Interagency Security Classification Appeals Panel (via the ISOO and coordinated by the Director, OSP). The lack of such approval shall result in the automatic declassification of the records.

17. Freedom of Information Act/Privacy Act Requests

DO/bureaus shall process requests for records containing classified information that are submitted under provisions of the Freedom of Information Act (FOIA), as amended, and the Privacy Act of 1974, as amended, in accordance with those Acts. FOIA review is similar to examination of classified information under the mandatory, systematic, and automatic review processes. When a request is submitted under both mandatory declassification review and the FOIA, the requester shall be required to select one process or the other. If the requester fails to specify, the request will be treated as a FOIA unless the requested materials are only subject to mandatory declassification review.

FOIA exemption (b)(1) protects classified material specifically authorized under criteria established by Executive Order to be kept secret in the interest of national defense or foreign relations of the United States that is, in fact, properly classified. The fact that records are classified does not qualify the information for automatic withholding under the FOIA. DO/bureau reviewers must examine subject records and declassify (in full or in part) those sections (of currently and properly classified records) that do not warrant continued classification. Actual release of newly declassified records might be subject to other FOIA exemptions; release should be determined by reviewers in consultation with subject matter experts, security, disclosure, legal and records management officials.

Treasury/bureaus will neither confirm nor deny the existence or nonexistence of requested records when the fact of their existence or nonexistence is itself classified under E.O. 13526 or under a prior Executive Order. Classified information that has been leaked to, or published by the news media, or otherwise made available to the public is not automatically declassified. Information is not considered in the public domain unless it has been officially disclosed and released by a U.S. Government official with authority to do so.

Whenever DO/bureaus receive a request for documents in their custody containing information originally classified by another agency, or discover such documents in the process of conducting mandatory, systematic or automatic declassification reviews, they shall refer copies of any request and the pertinent documents to the originating agency for processing. They may, after consultation with the originating agency, inform the requester of the referral unless such association is itself classified. In such instance they will neither confirm nor deny the existence or nonexistence of such records. Disclosure officials, records management officials, and reviewers shall consult with appropriate DO/bureau security officials to ensure classified documents are properly safeguarded throughout the FOIA/Privacy Act process. The process includes applying required markings to reflect decisions on downgrading, declassification, and release. See Chapter III, Section 5, Paragraph 20 regarding reclassification of previously disclosed information after a FOIA request has been received and the required involvement of the Secretary, Deputy Secretary or Senior Agency Official.

18. Redaction Standard

Classified information may be subject to loss, compromise, or unauthorized disclosure if it is not correctly redacted using only approved methods that permanently remove the classified information from copies of the documents intended for release based on technical guidance, equipment and standards applicable for classified electronic and optical media issued by the National Security Agency. DO/bureaus shall redact documents that are the subject of an access demand unless the overall meaning or informational value of the document is clearly distorted by redaction. However, the specific reason for the redaction must be included. Information that is redacted due to a statutory authority must be clearly marked with the specific authority that authorizes the redaction.

19. Restricted Data and Formerly Restricted Data

Consistent with existing law and policy, the steps for safeguarding restricted data (RD) and formerly restricted data (FRD) information vary according to the sensitivity of the information involved and whether the information is still classified. Records containing RD and/or FRD, e.g., classified nuclear weapons information require continued protection to prevent being misused or causing harm to the security of our nation or threatening public safety. These records include chemical, biological, radiological, and nuclear weapons information within classified documents, previously unclassified or declassified documents and sensitive but unclassified documents.

DO/bureaus shall avoid, to the extent practicable, commingling RD and FRD with information classified under the Order in the same document. When it is not practicable to avoid such commingling, marking requirements in the Order, the ISOO Directive and requirements in 10 CFR Part 1045, *Nuclear Classification and Declassification*, must be followed.

Chapter III Section 10 **Disseminating Classified Information** Updated 10/21/11

1. Dissemination

Classified information may only be shared with an individual who has the appropriate security clearance, at or exceeding the classification level of the particular information that the individual needs to receive to be able to conduct official U.S. Government business. The individual must also have the need-to-know the information, and must have signed a non-disclosure agreement and received contemporaneous training on protective requirements to safeguard classified information, the latter as referenced in Chapter III, Section 2.

Departmental Offices (DO)/bureau security officials shall ensure sufficient controls limit disclosure of classified information to only those persons authorized to receive it. Controls include those for physical/oral access, internal distribution, inventory, reproduction, and annually updating any automatic, routine or recurring dissemination rosters to distribute classified information.

2. Dissemination Controls

Classified information originated by DO/bureaus shall remain under the Department's control and shall not be removed from official premises without proper authorization.

a. *Sharing Among Government Branches.* When officials determine classified information is to be shared with the Legislative and/or Judicial branch of the Federal Government, DO/bureau security officials shall ensure the information is afforded equivalent protection to that provided within the Executive branch. Chapter III, Section 13 outlines the procedures for providing classified information to the Legislative Branch (U.S. Congress and U.S. Government Accountability Office (GAO)) and the Judicial Branch.

b. *Sharing Among Agencies (Modified 3rd Agency Rule).* Classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 1.4(a), E.O. 13526 are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information.

Classified information originating in one agency may also be disseminated by any other agency to which it has been made available: to a foreign government including any element of a foreign government, or an international organization of

governments or any element thereof in accordance with statute, EO 13526, 32 CFR Part 2001, or the direction of the President; or with the consent of the originating agency if otherwise permissible.

Documents created prior to June 25, 2010 shall not be disseminated outside any other agency to which they have been made available without the consent of the originating agency. The Secretary of the Treasury or the Senior Agency Official may waive this requirement for specific information that originated within that the Department of the Treasury. However, prior consent of the originating agency is not required when referring records for declassification review that contain information originating in more than one agency.

c. *Annual Review of Distribution Listings.* DO/bureau employees shall annually review all automatic distribution listings involving routine distribution and sharing of classified information. The update shall eliminate any recipients who no longer have the need-to-know or are no longer employed in the same position warranting continued receipt of classified information disseminated automatically.

3. Hand-carrying Classified (Hard-copy) Material

a. *Carrying Classified Information between DO/bureau Officials.* Hand-carrying classified information among and between DO/bureau officials is a routine business function. An important step in this process is ensuring that the recipient has the proper security clearance, the need-to-know, training to properly safeguard classified information, and has the capability to adequately store classified information.

b. *Carrying Classified Information within a DO/bureau Facility.* Within a DO/bureau facility, classified information may be hand-carried between offices by direct contact of the officials/employees involved or via cleared support staff. The information shall have the appropriate classified document cover sheet affixed to it and be placed inside a single, sealed, opaque envelope/file folder or security locking bag. The use of the envelope, folder or locking bag accomplishes the following:

- Makes it less obvious to casual observers, visitors, or un-cleared employees and contractors that the bearer is carrying classified information.

- Avoids associating a particular employee with his/her authorization to access classified information.

Such concealment is especially important whenever classified information is carried outside of DO/bureau controlled space within commercially-leased office buildings. Classified information shall not be delivered to unoccupied offices or rooms

c. *Carrying Classified Information while in Official Travel Status.* When personnel hand-carry classified information in official travel status, the physical transport shall avoid using non-U.S. flag aircraft or vessels. Classified information shall be taken across international borders only when absolutely essential and with the full knowledge of DO/bureau security officials. Every effort shall be made to use other authorized secure means for transport. If the U.S. Government's best interest requires hand-carrying classified information abroad, the following specific safeguards apply:

- Classified information shall be in the physical possession of the traveler at all times if proper storage in a U.S. Government facility is not available.
- Under NO circumstance shall classified information be stored in a hotel safe/room or locked in any vehicle, private residence, train compartment, detachable storage compartment, or other non-General Services Administration (GSA)-approved storage device.
- An inventory of all classified information shall be made prior to departure and a copy thereof retained by the traveler's office until the traveler's return – when all classified information shall be accounted for.
- Classified information shall not be read by the traveler or allowed to be viewed by unauthorized persons during the travel.
- First/business class travel may not be authorized when the justification is solely based on the need to read, prepare for, or study classified information.

NOTE: Hand-carrying SCI material while on official travel status is only as a last resort (i.e., there are no other options for transmittal under certain circumstances).

- Material will be double-wrapped.
- Material will be carried in a non-descript locking bag.
- Traveler will go from SCIF of origin to SCIF at final destination with NO stops authorized between (e.g., NO overnight stays in hotels).

4. Hand-carrying Classified Information on other Media

a *Laptops, Classified Disks.* The same requirements apply to classified information contained on laptops and disks as for hard-copy paper documents. Prior arrangements by the official DO/bureau traveler shall be made to ensure the classified laptop and classified information on disks are protected during the entire trip. Storage in U.S. Government controlled diplomatic facilities and advanced coordination with State Department officials are required.

Laptops for classified processing (and disks containing classified information) shall not be left unattended in hotel safes, rooms, conveyances, or stored overnight in U.S.-owned or foreign businesses either abroad or domestically. All laptops for classified processing and disks shall be continuously controlled by cleared, U.S. Government employees (24 hours per day, seven days a week) during official travel.

b. *Flash/Thumb Drives.* Flash/thumb drives are NOT approved for storing or transporting classified information.

c. *Secure Voice/Data Communications.* DO/bureau officials shall use secure communications; or Secure Telephone Equipment (STE) for conducting classified discussions. Communications include voice and data transmissions (facsimile or fax) under provisions established by Treasury systems security officials in Treasury Directive Publication (TD P) 85-01 Volume 1, Part 2.

5. Emergency Distribution

In an emergency, when it is necessary to respond to an imminent threat to life or in defense of the homeland, the Secretary of the Treasury or any designee may authorize disclosure of classified information (including that provided by another agency) to an individual or individuals who are otherwise not eligible for access. Such action shall be taken only in accordance with directives implementing E.O. 13526, and this section, minimizing the classified information that is disclosed under the emergency circumstances and the number of individuals who receive it.

Information disclosed under this provision shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. All such disclosures shall be reported promptly to the originator of the classified information via the Director, Office of Security Programs (OSP).

6. Classified National Security Information Program for State, Local, Tribal and Private Sector Entities

Executive Order 13549 established a program designed to safeguard and govern access to classified national security information shared by the U.S. Government with state, local, tribal and private sector (SLTPS) entities. The Department of Homeland Security serves as executive agent for this program. Policy provisions for access to and safeguarding of classified information (shared with SLTPS) shall generally not exceed the Secret level. When a sponsoring DO/bureau requests that a potential applicant has a demonstrated and foreseeable need for access to Top Secret information, such authorization shall be determined on a case-by-case basis by the Director, OSP. DO/bureau requests that a potential applicant has a demonstrated and foreseeable need for access to Sensitive Compartmented Information shall be made on a case-by-case basis by the Assistant Secretary for Intelligence and Analysis.

Upon execution of a non-disclosure agreement prescribed by the ISOO (for collateral information) or the Director of National Intelligence (for SCI) and absent disqualifying conduct as determined by the clearance granting official, a duly elected or appointed Governor of a State or territory, or an official who has succeeded to that office under applicable law, may be granted access to classified information without a background investigation in accordance with the implementing directive for E.O. 13549. This authorization of access may not be further delegated by the Governor to any other person.

7. Removal of Classified Information by Departing Employees

The access to, or removal of classified information by departing and former employees is governed by procedures contained in Treasury Directive (TD) 25-05 *The Freedom of Information Act* and TD 80-05, *Records and Information Management Program.* Documentary materials include Federally-owned information and material that meet the statutory definition of records, including such electronic communications.

8. Waivers Allowing Access to Classified Information

a. *Obtaining Waivers.* Access to classified information shall normally be granted only when it is essential to accomplish lawful U.S. Government purposes. Restrictions may be waived for those persons who:

- Are engaged in historical research projects. However, conferring historical researcher status does not include authorization to access or release foreign government information or another Federal agency's classified information.
- Previously occupied a policy-making position by appointment of the President of the United States or the Vice President of the United States.
- Served as President or Vice President.

b. *Granting Waivers.* A waiver may only be issued by the Secretary of the Treasury or the Department's Senior Agency Official (SAO). Either official must:

- Determine in writing that access is consistent with the national security of the United States.
- Take appropriate steps to protect classified information from unauthorized disclosure or compromise while ensuring that the information is properly safeguarded.

- Restrict access to former Presidential and Vice Presidential appointees to items the individual originated, reviewed, signed, or received while serving in that official capacity.

c. *Coordination.* All waivers will be coordinated with the Director, OSP to ensure access to classified information by historical researchers, former Presidential and Vice Presidential appointees, and to comport with Treasury policy, including the following:

- Provisions of TOs 25-05 and 80-05 and the national interest.
- Written agreement to safeguard classified information.
- Consent to having notes and manuscripts (in paper and electronic format) reviewed to ensure no classified information is contained therein. The review might entail degaussing equipment used in electronic processing or scrubbing affected memory storage to eliminate classified information from being inappropriately retained and accessible by unauthorized persons.
- Payment of fair and equitable fees for services such as search and/or review and copying, under the fee schedule in Chapter III, Section 9 for mandatory review, if required.

9. Sharing Security Equipment Combinations

Combinations to security equipment storing classified information are administratively classified to the highest level of the classified information stored within the security equipment. Before an individual may be provided any security equipment combination, the sharing employee must first verify the individual's security clearance and his/her need-to-know the information stored, or to be stored, within the security equipment. An individual's security clearance level shall be verified through DO/bureau personnel security channels. The individual's need-to-know must be determined by his/her supervisor who shall also notify DO/bureau security officials when cleared personnel depart so that combinations to security containers storing classified information are not lost/forgotten potentially resulting in costly drilling/repairing of the equipment.

Security container/safe custodians are responsible for ensuring any newly authorized person's name is added to (updating) Standard Form (SF) 700, *Security Container Information.* This information shall be relayed to the DO/bureau security official responsible for maintaining all security equipment combination records.

DO/bureau security officers shall periodically review SF 700 records of combinations to ensure the information (and the actual combination) is accurate with respect to particular security storage equipment. Office occupants shall assist and cooperate with DO/bureau security officers in conducting inventories of security equipment combinations.

Chapter III Section 11 — **Packaging, Reproducing, and Transmitting Classified Information** — Updated 10/21/11

1. Introduction

This section establishes the physical security requirements for properly handling and safeguarding classified information under Executive Order (E.O.) 13526 and Information Security Oversight Office (ISOO) Directive at 32 CFR Part 2001). The focus is on packaging, reproduction and transmitting classified information in the course of official U.S. Government business.

2. Packaging Classified Information

All classified information packaging shall be of sufficient strength and durability to:

- Provide security protection while in transit.
- Prevent items from being damaged.
- Preclude inadvertent access to the contents.
- Detect possible tampering, sealed with tamper-resistant filament tape.
- Ensure delivery in a timely manner.

Hard-copy (paper) classified documents that are hand-carried outside of a DO/bureau facility shall be prepared as follows:

- Have the proper cover sheet affixed.
- Be enclosed in opaque inner and outer protective envelopes/covers that shall provide reasonable evidence of tampering and which conceal the contents.

The innermost envelope/cover shall be sealed and clearly marked with the highest level of classified information being carried (including any appropriate warning caveats or restriction notices) and the names and addresses of the sender and recipient.

The outermost envelope/cover shall identify the names and addresses of the sender and recipient; however, there shall be no indication that the contents are classified. A locked briefcase, attaché, or portfolio (or security locking bag) may serve as the outer envelope/cover in the same manner used for material sent via diplomatic pouch.

If the material is too large for envelopes or similar wrappings, the material shall be enclosed in two sealed opaque boxes. Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may also be considered the outermost protective cover. Classified information delivered in diplomatic or other type pouches by other Federal agencies and receipted to DO/bureaus and delivered to the intended recipient (leaving a single layer of protection) shall not be considered a security violation for purposes of proper packaging/safeguarding.

Packaging requirements for safeguarding classified information during transit shall not eliminate the need for screening mail or packages to detect or deflect possible hazardous agents being introduced into DO/ bureau controlled space or facilities. Employees or contractors who screen incoming mail and packages shall have at least a Secret-level security clearance.

Within DO, an Access Control Register (See Attachment 1), produced on blue stock, shall initially be used to identify mail handlers who are authorized to open incoming classified mail for screening prior to delivery. Once the mail or a package is determined to be safe for internal delivery, it shall receive continuous protection until actually carried to its destination and appropriately delivered. Such screened items shall be internally hand-receipted to authorized recipients using the blue Access Control Register. No classified items may be left inside an unoccupied office or room for later retrieval of the annotated Access Control Register. Mail handlers will retain custody of the Access Control Register on file as evidence of each successful delivery. Bureau security officials may adopt use of the same Access Control Register for classified information in the mail screening process for their use, as warranted.

3. Reproduction Controls for Classified Information

Use of technologies to prevent, discourage, or detect unauthorized reproduction (including specialized paper, copy numbering, and distribution restrictions, as might be warranted for particular classified information) are encouraged. Reproduction controls shall ensure classified information is protected in its entirety during the copying process. Such reproduction shall only be made by cleared DO/bureau employees and contractor personnel who are fully knowledgeable of classified handling procedures. Copiers are like computers and much depends on whether or not an individual copier is networked or a stand-alone or is equipped with a removable hard drive and also if it has been approved by security officials for classified or unclassified reproduction. Non-networked copiers may be approved for classified information depending on user need, the physical location of the machine and security officials' approval. Some copiers are equipped to wipe, erase, or clear all the information after each use or may not have memory retention capability. This makes the old custom of running extra pages unnecessary on such copier machines. Check with the equipment manufacturer for information on individual copier capabilities. Only copiers specifically approved for classified reproduction may be used for such reproduction, and only under the following procedures:

- Do not leave a copier machine or facility without ensuring the originals are retrieved along with all reproductions – even damaged or flawed copies.

- Destroy unusable copies by burning, mulching, or shredding. No record is required.

- Only use burn-bags to dispose of Secret and Confidential information.

Note: Copying sensitive compartmented information (SCI), special access program (SAP) information, and special access required (SAR) information outside of Special Security Officer (SSO) channels is not authorized.

a. *Copy Machines.* Copy machines approved for classified reproduction shall be labeled as such – at a minimum using *Standard Form Labels 706 (*orange for Top Secret) *707* (red for Secret) and *708(* blue for Confidential) and indicating any restrictive caveats that might be applicable. One or more such labels shall be affixed to copier equipment.

b. Additional "original" copies may be made on printers connected to the Treasury Secure Data Network (TSDN), restricted to only the Secret and Confidential levels. The following types of copy machines may not be used for classified information:

    - Networked copying machines on any *unclassified* local area network.

    - Copiers equipped with remotely accessible memory, diagnostic, or maintenance capability.

b. *Restrictions on Reproduction.* Copying Top Secret information requires approval of the originator (including non-DO/bureau originators) unless reproduction is supporting the review for declassification. Secret and Confidential information has no such restriction except that copying shall be accomplished only as needed for operational efficiency. All copies shall be subject to the same storage, handling, access, destruction, and accountability controls as the originals.

NOTE: Unusable copies of SCI material will be placed in burn bags and collected for shredding.

4. Transmittal of Classified Information within the U.S. Government

Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified

information.

a. *Top Secret Information.* Transmittal of Top Secret information outside of a DO/bureau facility shall only be accomplished in person-to-person contact by specifically cleared employees; by State Department diplomatic pouch; by a messenger-courier system authorized for that purpose, e.g., the Defense Courier Service (DCS) or authorized secure communications. Top Secret information may not be sent via the U.S. Postal Service. The DCS is intended as a means to securely transport Top Secret information, but SCI may be included if going to the same destination. The DCS shall not be used when only Secret or Confidential information needs to be transmitted.

NOTE: Transmittal of SCI material within the U.S. Government outside of DO/bureaus will be accomplished via courier service in a point-to-point manner.

b. *Secret Information.* DO/bureaus may not send Secret information via certified mail. The procedures for transmitting Secret information depend on where it was originated and its destination. Transmittal of Secret information shall be accomplished within and between the fifty States, District of Columbia, and the Commonwealth of Puerto Rico by any of the following methods:

- One of the means authorized for Top Secret information (subject to the above DCS restriction).
- The U.S. Postal Service (USPS) Express Mail or USPS Registered Mail - but the waiver of signature and indemnity block (item 11-B) on the label may not be used.
- Cleared commercial carriers/messenger services.
- Protective services provided by U.S. air or surface commercial carriers.

Within other areas, Secret information may be sent by any of the following four methods:

- USPS through Military Postal Service facilities provided the information does not at any time pass out of U.S. citizen control and/or through a foreign postal system.
- Under escort of appropriately cleared personnel aboard U.S. Government-owned and U.S. Government-contract vehicles or aircraft.
- Ships of the U.S. Navy, civil service manned U.S. Naval ships, and ships of U.S. registry.
- Operators of vehicles, captains or masters of vessels, and pilots of aircraft

who are U.S. citizens, and who are appropriately cleared, may be designated as escorts.

Under exceptional circumstances and when an urgent requirement exists for overnight delivery within the United States and its territories, Secret information may be sent by an authorized holder of the General Services Administration (GSA) contract for overnight delivery for the Executive Branch as long as applicable postal regulations are met. DO/bureaus shall not establish a standard or common practice of relying on GSA contract carriers for overnight classified delivery.

Note: Classified Communications Security Information, North Atlantic Treaty Organization (NATO), and foreign government information may not be sent via GSA contract overnight delivery.

Overnight delivery servicing carriers shall be U.S.-owned/operated and shall provide automated, in-transit tracking of the classified information along with package integrity during transit. Service providers shall cooperate with U.S. Government inquiries in the event of a loss, theft, or possible compromise of classified information. DO/bureaus are responsible for ensuring an authorized person is available to receive the delivery and to verify the correct mailing address. Accordingly, no signature release on the receipt label is authorized.

Further, neither external (street-side) collection boxes nor internal or unmanned collection boxes may be used to drop off classified information for later pick-up. Transfer of custody to a representative of the GSA-contract carrier for overnight delivery must always be done person-to-person.

c. *Confidential Information.* Transmittal of Confidential information shall be by any of the methods established for Secret information. DO/bureaus shall not send Confidential classified information via certified mail.

5. Classified Information to Foreign Governments

Transmission of U.S. classified information to foreign governments shall take place between designated government representatives using government-to-government transmission methods or through channels agreed to by the national security authorities of the two governments. When classified information is transferred to a foreign government or its representative a signed receipt is required; oral discussions of classified information do not require receipt acknowledgment. Coordination with the Special Security Office, Office of the Assistant Secretary for Intelligence and Analysis is required.

6. Receipt for Classified Information

DO/bureaus shall use Treasury Department Form (TD F) 15-05.8, *Receipt for Classified*

Information, to receipt and account for classified information.

7. Couriers

DO/bureau couriers and other authorized persons with a frequent and recurring need to hand-carry classified information shall provide constant and continuous protection while the material is in their custody. Only direct, point-to-point deliveries are authorized. Persons designated to be couriers shall also carry on their person a Treasury courier card issued by DO/bureau security officials to verify their courier status. Designations of couriers and the required training explaining their responsibilities as a courier shall be formally documented. (See Chapter V Section 6).

Attachment 1

CLASSIFIED (SECRET, CONFIDENTIAL or RESTRICTED)
Unclassified upon removal of attachment(s)

ACCESS CONTROL REGISTER
(Produced on Blue Stock - Do Not Photocopy)

WARNING NOTICE: The attached information is classified SECRET, CONFIDENTIAL or contains Foreign Government RESTRICTED information. It must be handled in accordance with established Treasury security procedures and may not be reproduced except by the receiving office as may be necessary for official purposes. All employees who handle the attached information at any time in the screening or delivery process shall be identified below. Type or print legibly in ink.

UNAUTHORIZED DISCLOSURE IS SUBJECT TO CRIMINAL SANCTIONS

Employee's Printed Name	Signature	Office	Date

Chapter III
Section 12

Airline Transport of Classified Information

Updated
6/17/11

1. Introduction

Security arrangements with the Transportation Security Administration (TSA) and U.S. commercial airlines are required whenever Departmental Offices (DO)/bureau travelers must hand-carry classified information essential to conducting official U.S. Government business. The arrangements are to protect the traveler, to prevent loss or possible compromise of the information, and to maintain the integrity of the screening process established by TSA and the Department of Homeland Security (DHS). Practices and procedures in this section shall also be used for sensitive information when it must be hand-carried on airlines for official business purposes.

a. *Non-U.S. Airlines.* Use of non-U.S. (foreign registry) airlines for transport of classified information is not authorized.

b. *U.S. Military Aircraft.* Use of U.S. military aircraft for official travel by DO/bureau employees, as provided by the Department of Defense (DOD), shall be coordinated with appropriate DOD security officials and governed by military protocol.

c. *U.S. Commercial Airlines.* Classified information shall not be carried aboard commercial airlines unless DO/bureau security officials have been notified in advance that the following conditions are true:

- The information is essential to conduct official business and is not already available at the traveler's destination.
- There is insufficient time and no other available secure means of transmission to achieve operational DO/bureau objectives.
- The size, weight, and physical configuration permit it to be carried on the traveler's person or qualify as carry-on baggage.
- The traveler abides by the procedural requirements in paragraphs 2 and 3 of this section.

d. *Privately-Owned Aircraft of U.S. Registry.* Use of privately-owned aircraft of U.S. registry shall be avoided unless this is the only available means of transporting classified information, subject to time, security and carry-on baggage constraints.

2. Basic Requirements

DO/bureau travelers are encouraged to use a driver's license for photo identification purposes for normal official travel to more readily blend in with other passengers. However, official U.S. Government identification is required when the traveler is hand-carrying classified information to establish the DO/bureau employee's bona fides with TSA screening officials as might be necessary in the screening process.

When classified information must be hand-carried by official DO/bureau travelers, DO/bureau security officials shall coordinate in advance with TSA/DOD and U.S. airline carrier representatives to develop mutually satisfactory arrangements.

a. DO/bureau travelers may be designated as couriers and issued courier cards/letters under procedures in Chapter V, Section 6. To avoid possible damage to high-speed films and other forms of sensitive electronic/magnetic media, couriers shall exercise precautions when carrying such media through baggage screening detection equipment.

b. *Opening/Reading Classified Information.* TSA/DOD screening personnel are not permitted to open, view or read classified information in the traveler's custody and DO/bureau travelers shall not authorize classified information to be opened, viewed, or read by unauthorized persons. Travelers are also precluded from opening or reading classified information on military or any other aircraft. Travelers shall promptly notify the Director, Office of Security Programs (OSP), whenever classified information is subject to being opened, viewed, or read incident to their official travel.

3. Classified Information Screening Procedures

Classified information in hard copy paper format, electronic, or other forms of media shall be sealed in opaque inner and outer envelopes. The inner envelope shall be marked with the assigned classification level and addresses of the sender and recipient. The outer envelope shall have both addresses but no indication of classification. DO/bureau official travelers who must hand-carry classified information shall rely on the following procedures to exempt U.S. Government classified material from screening checkpoint inspection:

a. *Exempt Screening.* Upon arrival at the screening checkpoint, the traveler carrying U.S. Government classified material must present to a TSA screening official:

(1) DO/bureau-issued photo identification.

(2) A valid courier letter/card substantiating his/her authorization to hand-carry classified information.

The TSA screening official will verify that a traveler's letter/card includes each of the following:

(1) The full name of the individual and his/her employing DO/bureau organization.

(2) A date of issue and expiration date.

(3) The name, signature, and phone number of the DO/bureau official issuing the letter/card to confirm the bearer's letter/card authorization.

Once the TSA screening supervisor has verified the traveler's authorization to carry classified material, the screening TSA supervisor will exempt only the U.S. Government classified material from any form of inspection. The courier and his/her personal accessible property shall be screened in the same manner as the traveling public. The U.S. Government classified material must remain within the courier's line of sight at all times during the screening process. Any "loss of sight" control shall be reported to DO/bureau security officials as soon as possible.

If an individual claims to have U.S. Government classified material but does not present a valid courier letter/card and Government-issued photo ID, the material may not be permitted into the sterile area unless it has been properly screened.

b. *Routine Screening.* If the sealed envelope is in a briefcase or other carry-on luggage, the case/luggage shall be offered for inspection/screening. TSA screening officials may be permitted to physically inspect the inside of the briefcase/luggage and examine the sealed envelope by flexing, feeling, weighing, etc., but not by opening. Classified information in sealed package containers unsuited to processing because of the size, weight, or other physical characteristics shall also be screened to TSA satisfaction. DO/bureau travelers are also subject to similar DOD screening on military aircraft.

c. *Further Screening.* If the TSA screening official is not satisfied, the traveler shall request any further screening be conducted away from the public area. This is to avoid subjecting the sealed envelope or package and the traveler to public scrutiny/observation.

d. *Biochemical Screening.* TSA/DOD screeners are permitted to use biochemical detection devices but only in the presence of the traveler.

- If no alarm results, the sealed envelope or package requires no further examination.

- If an alarm does result, the traveler will be denied boarding and should expect to be detained by TSA/DOD officials until the matter can be resolved. In such occurrence, DO/bureau security officials must be immediately contacted to respond to TSA/DOD inquiries.

4. Bulky or Oversized Classified Package Screening Procedures

If the material is too large or bulky it shall be enclosed in two opaque sealed boxes. The intention is to double-wrap the material similar to protecting classified information in standard sized U.S. Government envelopes. Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may also be used, in which case the outermost protective enclosure replaces the second sealed box.

All packaging shall be of sufficient strength and durability to:

- Provide security protection while in transit.
- Prevent items from being damaged.
- Preclude inadvertent access to the contents.
- Reveal possible tampering by being sealed with tamper-resistant filament tape.
- Ensure delivery in a timely manner.

Bulk package shipments containing classified information are also subject to the same TSA screening regimen outlined in part 2, above.

Chapter III Section 13 **Providing Classified Information to the Legislative and Judicial Branches** Updated 6/17/11

1. Introduction

This section establishes procedures for providing classified information to the Legislative Branch (U.S. House of Representatives, U.S. Senate and the Government Accountability Office (GAO)), and the Judicial Branch (under the Classified Information Procedures Act (CIPA)), or for grand jury purposes by Departmental Offices (DO)/bureau employees. These procedures shall also be used as guidance by DO/bureaus providing sensitive information to Congress, GAO, and the Judiciary.

2. Requirements for Release of Classified Information

Release of classified information to Congress and GAO is predicated on affirmation by DO/bureau officials responsible for safeguarding classified information that such information may be shared with the Legislative Branch. Such information may be presented only in executive or closed sessions of congressional committees or to authorized and cleared congressional recipients or GAO employees.

Release of classified information to the Judiciary under the CIPA or for grand jury purposes should be in conjunction with DO/bureau classified information possibly pertinent to a criminal proceeding and to ensure protection of classified equities contained therein.

Only classified information for which DO/bureaus is responsible shall be eligible for release. Non-Treasury-originated materials, including information DO/bureaus derivatively classified, shall not be released without prior written approval from the agency/department that originated the information. Release determinations to Congress, GAO, and the Judiciary shall be made in consultation and/or coordination with DO/bureau security and legal officials.

3. Responsibilities of DO/Bureau Security Officials

Security procedures for properly handing classified information shall be followed to ensure the information is adequately protected against unauthorized disclosure. DO/bureau security officials shall advise policy/program level officials and legal counsel on the physical exchange, transmission, and packaging requirements to protect:

- Hard-copy classified paper documents.
- Soft-copy classified electronic documents (via e-mail or on disk).

- Oral discussions, including secure phone or facsimile, person-to-person, or in meetings with multiple individuals.

4. Classified Information Intended for the United States Senate

a. Classified information intended for delivery to the U.S. Senate during normal business hours (approximately 9:00 AM to 5:00 PM) shall be hand-carried to the Capitol Building for the Office of Senate Security (OSS). The OSS regulates how classified information is handled by all Senate offices/employees and it maintains the Senate's classified information document registry. Senators and offices who receive or store classified information, or who employ staff holding a security clearance, are responsible for following OSS procedures. The OSS is accessible via the Visitor Center entrance on the east side of the Capitol building, within Room SVC-217, and can be reached at telephone number (202) 224-5632.

b. Top Secret information may only be hand-carried to OSS. Secret and Confidential information may be delivered to OSS or hand-carried directly to the U.S. Senate (only with prior Department of the Treasury coordination) by an authorized courier to one of the following offices:

- The Committee on Appropriations, Room SD-119, Dirksen Building.
- The Committee on Armed Services, Room SR-228, Russell Building. This office will accept only receipted classified packages addressed to the Chairman, the Ranking Minority Member, or to individual Committee staff members. Classified packages addressed to all others shall be delivered to OSS.
- The Defense Appropriations Subcommittee, Room SD-119, Dirksen Building.
- The Committee on Foreign Relations, Room SD-423, Dirksen Building.
- The Committee on Intelligence, Room SH-211, Hart Building.

Under no circumstances shall classified information be delivered directly to a Senator's personal office. A multiple-copy receipt shall be included with all classified packages hand-carried to the U.S. Senate.

c. By previous arrangement, Senate employees may be granted access to collateral classified information by the Office of the Secretary of Defense (OSD) following an investigation conducted by the Federal Bureau of Investigation (FBI) or the Office of Personnel Management (OPM). The Central Intelligence Agency (CIA) may grant access to sensitive compartmented information (SCI), as warranted. Only their employing Senator may request that an employee be investigated for

access to classified information. According to OSS, no one on a Senator's personal staff is allowed SCI access. Neither DO nor are any Treasury bureaus authorized to investigate Senate employees for access to classified information. Any requests for access to DO/bureau classified information from Senate sources shall be forwarded to and coordinated with the OSS. Verification of clearances shall be obtained via normal personnel security channels.

d. Security procedures for screening all Senate-destined mail have resulted in classified information intended for OSS no longer being able to be sent via the U.S. Postal Service's (USPS's) first-class, registered mail, USPS express mail or GSA-approved overnight carrier service. All classified information for OSS must now be hand-carried by cleared DO/bureau employee/messenger. Advanced arrangements with OSS are necessary given established security controls and/or changes in the national threat level affecting access to the Capitol Building.

e. Classified material shall be packaged in opaque, double envelopes in the same manner as other classified information sent via the U.S. mail. However, the inner envelope shall be addressed to the specific Ranking Majority Member and/or Ranking Minority Member, as appropriate; and the outer envelope shall be addressed to the OSS. Upon receipt, OSS will arrange for delivery, accountability, review and storage with the assigned security manager in respective Senate committee offices.

5. Classified Information intended for the United States House of Representatives

a. Classified information intended for delivery to the House of Representatives during normal business hours (approximately 9:00 AM to 5:00 PM) shall be hand-carried directly to the Ranking Majority Member and/or Ranking Minority Member, as applicable, but only upon verifying adequate storage capability for classified information. Deliveries to Congressional Committees, subcommittees, and individual Member's offices and staff are not authorized.

b. The House of Representatives does not operate a centralized security office such as that of the Senate, therefore, no central depository exists for delivery and receipt of classified information.

c. In all instances, the identity and security clearance of intended House of Representatives employee recipients must be verified in advance of any delivery being made. Such coordination shall be made via normal DO/bureau personnel security channels with the House Sergeant-at-Arms, Office of the Information Security Section, U.S. Capitol Police. That office is located in Room H-124, The Capitol, and can be reached at telephone number (202) 225-2456.

d. Security clearances issued to House of Representatives employees in the same manner as Senate employees. Such clearances shall be honored; provided the investigation in support of the clearance is current and written verification is obtained. DO/bureaus are not authorized to investigate House of Representatives employees for access to classified information. It is the responsibility of the employing House Member to initiate such action with the House Sergeant-at-Arms.

e. Classified information destined for the House of Representatives must be hand-carried by cleared DO/bureau employee/messenger to the House Sergeant-at-Arms and may no longer be sent via the USPS's first-class, registered mail, USPS express mail or General Services Administration (GSA)-approved overnight carrier. Advanced arrangement with the House Sergeant-at-Arms is required given established security controls and/or changes in the national threat level affecting access to the Capitol Building.

e. Classified material shall be packaged in opaque, double envelopes in the same manner as other classified information sent via the U.S. mail. However, the inner envelope shall be addressed to the specific Ranking Majority Member and/or Ranking Minority Member, as appropriate. The outer envelope shall be addressed to the House Sergeant-at-Arms. That office will assist in directing the DO/bureau cleared employee/messenger to deliver the packaged classified information and verify potential recipients have required storage capability.

6. Classified Information Released to General Accountability Office

Requests for release of Treasury classified information to the Government Accountability Office (GAO) shall be coordinated by the responsible DO/bureau security official with the Director, GAO Security and Safety (SAS), 441 G Street NW, Room 1T23, Washington, DC 20548, at telephone number (202) 512-4700. SAS can verify security clearance status and the need-to-know of intended GAO recipients and act as a central repository, when necessary, for classified information transmitted or hand-carried to GAO.

7. Acknowledging the Receipt of Classified Information

Treasury Department Form (TD F) 15-05.8, *Receipt for Classified Information,* shall be affixed to (but not inside) the inner envelope of all classified information provided to the Senate, the House of Representatives, GAO, and the Judiciary. The latter shall be in coordination with the Court Security Officer designated by the Department of Justice under the *Classified Information Procedures Act.* Classified document receipts are required for all Top Secret, Secret and Confidential information released to the Legislative and Judicial branches. Tracer actions for unreturned receipts for classified information shall be initiated with the OSS, the House Sergeant-at-Arms, the Director, GAO Security and Safety, or the Court Security Office, as appropriate. Whenever

classified information is provided to the Senate, the House of Representatives, GAO, and/or the Judiciary, respectively, each copy shall be individually numbered and the accompanying receipts annotated to reflect each recipient.

8. Notification to the Office of Legislative Affairs

Treasury's Office of Legislative Affairs shall be notified whenever classified information is provided to the Senate, the House of Representatives and/or GAO. Such notice shall include identification of the respective Ranking Majority Member, Ranking Minority Member, name of the respective Committee(s), and/or identity of the GAO office/recipient, as appropriate, for which the information is destined, and the generic unclassified subject of the information.

9. Coordination with the Legal Division

The Legal Division is responsible for alerting U.S. prosecutors whenever DO/bureau-originated classified information might be pertinent to a criminal proceeding or for grand jury purposes. The Legal Division shall coordinate with DO/bureau security officials to ensure classified information is properly packaged, handled, transmitted and accounted for. This includes liaison with the Court Security Officer under the Classified Information Procedures Act for safeguarding classified information.

Chapter III
Section 14

Release of Official Treasury/Bureau Information

Updated
6/17/11

1. Introduction

The release of official information, (classified, sensitive, or non-sensitive) may only be accomplished via specific authority under Departmental Offices (DO)/bureau regulations governing official information. DO/bureau officials are responsible for reviewing official documents (regardless of the format) and determining what part or parts (if any) may be released, when, and how.

2. Declassification

Declassification is the authorized change in the status of information from classified to unclassified and includes application of appropriate markings to reflect this change in status and notification to authorized recipients of the change in classification. The premise is that information shall be declassified as soon as it no longer meets the standards for continued classification under Executive Order (E.O.) 13526, and with due respect to protecting foreign government information as well as confidential sources.

In some cases the need to protect classified information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the Secretary of the Treasury or the Department's Senior Agency Official (SAO), via the Director, Office of Security Programs (OSP). Either official will determine at their discretion whether the public interest in disclosure outweighs the damage to the national defense or foreign relations of the United States that could reasonably be expected from disclosure. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural rights subject to judicial review.

3. Emergency Release of Classified Information

Emergency release of classified information is permitted under Section 2001.52 of the ISOO Directive by the Secretary of the Treasury; or that official's designee, when it is necessary to alert or respond to an imminent threat to life or in defense of the homeland. Such emergency disclosure of classified information to individuals not otherwise eligible for access to classified information does not automatically result in declassification. The amount of classified information disclosed must be limited in scope and to the minimum number of individuals. Additionally, transmittal shall be via approved Federal Government channels by the most secure and expeditious method or means deemed necessary when time is of the essence with instructions about what specific information is classified and how it should be safeguarded. Within 72 hours of the disclosure or the earliest opportunity that the emergency permits, but no later than 30 days after the

release, the disclosing authority must notify the originating agency of the information and provide the following:

a. Description of the disclosed information.
b. To whom the information was disclosed.
c. How the information was disclosed and transmitted.
d. Reason for the emergency release.
e. How the information is being safeguarded.
f. Description of the briefings provided and a copy of the non-disclosure agreement signed.

4. Declassified Information

When information is declassified, the document (regardless of format) must be appropriately marked to reflect this change in status. Reasonable efforts must be made to notify known recipients of the change in classification status. Declassified information might have lingering sensitivity depending on either the nature or source of the information. If so, it shall be reviewed by DO/bureau program/policy-level officials in consultation with legal/security officials and especially with respect to all possible intelligence aspects. In the latter instance if end users are uncertain about potential release, they shall consult with the Office of Assistant Secretary for Intelligence and Analysis (OIA) for guidance.

5. Decontrol of Information

Decontrol is the determination that sensitive information no longer merits protection and might be subject to possible release. The extent to which certain information may be withheld from release under the FOIA/Privacy Act depends on whether the information meets one or more specific exemptions in those Acts. (See http://www.treas.gov/foia/guidance.html).

6. Disposition of Information

Classified and sensitive information that is no longer needed in current working files or for reference/record purposes shall be processed for disposition in accordance with records management and disclosure regulations governing the disposal of Federal records. Release-ability determinations shall be made by program or policy-level officials in consultation with records management officials and/or disclosure/security and legal officials depending on the nature of the information. Except for justified emergency release, classified information must be formally declassified in order for it to be released to the public. Release of declassified or sensitive information, under specific authority, is governed by one or more of the processes illustrated in the chart below.

7. Warning Notice

Where a determination has been made that particular DO/bureau information meets an exemption under the FOIA or the Privacy Act, it shall be annotated in a warning notice affixed to the document as meeting a specific exemption. Individual portions or paragraphs shall also be marked to indicate the information to which the warning applies. Non-exempt portions or paragraphs are releasable. DO/bureau employees, consultants and contractor personnel shall refrain from the application of *carte blanche* exemption-markings by rote application.

8. Requests by Departing and Former Employees to Access or Remove Documentary Materials.

Treasury Orders 25-05 and 80-05 provide guidance on requests by departing and former employees to access or remove documentary materials from DO/bureau custody.

Processes Used to Release Information

Process	*Type of Record*	*Contact Offices*	*Further Review or Approval*
FOIA[1]	Unclassified/SBU	Program Office (PO)	Disclosure
	Classified	PO Office of Security Programs (advisory/guidance only)	Disclosure
Privacy Act[1]	Unclassified/SBU	PO	Disclosure
	Classified	PO OSP (advisory/guidance only)	Disclosure
TO 25-05 and 80-05[2]	Unclassified/SBU	PO/Disclosure	Disclosure
	Classified	PO OSP (advisory/guidance only)	Disclosure
"Touhy"[3]	Unclassified/SBU	PO/Legal Division	Legal Division
	Classified	PO/OSP/Legal Division	Legal Division
Classified Information Procedures Act[4]	Classified	PO/OSP/Legal Division	Justice Department
EO 13526 Mandatory Review[5]	Classified	PO OSP (advisory/guidance only)	Office of Security Programs
EO 13526 Systematic Review[5]	Classified	PO/Records Management OSP (advisory/guidance only)	---
EO 13526 25-Year Automatic Declassification[5]	Classified	PO/Records Management OSP (advisory/guidance only)	Other agencies for non-Treasury equities

[1] Freedom of Information Act/Privacy Act, as amended.
(31 CFR Part 1, Subparts A, C and B "other disclosure provisions)

[2] Treasury Order 25-05, *The Freedom of Information Act* and Treasury Order 80-05 *Records and Information*

Management Program.

[3] "Touhy" regulations, at 31 CFR 1.11, release of information in legal proceedings.

[4] Classified Information Procedures Act – criminal prosecutions.

[5] EO 13526: Mandatory Review, Systematic Review, 25-Year Automatic Declassification.

Chapter III
Section 15

Top Secret Control Officers and Security Contacts

Updated
6/17/11

1. Introduction

Each Departmental Office (DO)/bureau that originally and derivatively classifies or otherwise handles Top Secret information shall designate in writing a primary and alternate official to be their organization's Top Secret Control Officer (TSCO). DO/bureaus shall annually notify the Director, Office of Security Programs (OSP), in writing at the beginning of each fiscal year, of the identity of the individuals (primary TSCO and alternate) assigned this function by name/phone/email address within their organization.

2. DO Responsibilities

Within DO proper, the primary TSCO function is established in the Office of the Executive Secretary (for collateral Top Secret information) and in the Office of the Assistant Secretary for Intelligence and Analysis (for Sensitive Compartmented Information (SCI)). Both offices shall establish a process of recording and receipting for Top Secret information to DO/bureau policy-level client offices responsible for particular issues and activities and may re-delegate the TSCO function in writing to one or more subordinate components.

Designated TSCO employees must have a Top Secret security clearance and receive training from DO/bureau security officials on their TSCO responsibilities. Additional training shall be provided by the Office of Intelligence and Analysis for employees assigned TS/SCI TSCO responsibilities.

The Office of the Executive Secretary and the Office of the Assistant Secretary for Intelligence and Analysis (OIA) shall maintain the official log of all Top Secret information they receive, store, and assign to particular offices for information purposes or for appropriate action and/or response. This includes establishing and maintaining the numbering system to further account for Top Secret information held within DO.

3. Treasury Bureau Responsibilities

Bureaus shall establish the TSCO responsibilities within their security (or emergency preparedness function) depending on the volume and nature of Top Secret information held within their bureau. Designated employees must have a Top Secret security clearance and receive training from bureau security officials on their TSCO responsibilities. Additional training shall be provided by the Office of Intelligence and Analysis for employees assigned TS/SCI TSCO responsibilities.

4. Forms for Recording

Treasury Department Form (TD F) 15-05.4, *Top Secret Document Control Register*, shall be the primary form used to account for Top Secret information. The TD F 15-05.4 is available at http://intranet.treas.gov/security/forms. Instructions for completion are included on the form. Additionally, TD F 15-05.10, *Top Secret Document Record*, shall be affixed to all Top Secret documents. The TD F 15-05.10 in printed on green stock and shall not be photocopied in such a manner that the intentional color-coding is omitted. The TD F 15-05.10 is in addition to the Top Secret Document Record.

5. Top Secret Control Officer Responsibilities

Each TSCO or alternate shall perform the following:

- Initially receive and open all Top Secret information within their organization. This includes Top Secret information delivered to DO/bureaus by outside courier and/or brought back to DO/bureaus by an employee, except that SCI must be delivered directly to the Office of Intelligence and Analysis. In the former instance, all incoming Top Secret information must be brought to (and logged in by) the TSCO or alternate by the next business day.

- Maintain current accountability records of Top Secret information received within their office or bureau and attendant supply of Top Secret document forms.

- Ensure Top Secret information is properly stored and that such information under their personal custody is destroyed, when required, under two-person control and documented.

- Strictly follow prohibitions against reproduction of Top Secret information.

- Conduct an annual physical inventory of Top Secret information within the immediate organization along with the designated alternate TSCO or another Top Secret cleared employee or contractor (if appropriate). The results shall be provided in a written report to the Director, OSP, signed by the TSCO and the witnessing individual. If there are unaccountable documents, the report shall include a plan of action with identifiable milestones and dates for resolving whatever circumstances caused material to be lost or missing.

- Downgrade, declassify, retire, or destroy Top Secret documents, as appropriate to the markings and/or other caveats on such information.

- Affix a TD F 15-05.10, *Top Secret Document Record*, and Standard Form (SF) 703, *Top Secret Document Cover Sheet*, to all copies of Top Secret information leaving the immediate office/bureau prior to delivery to other offices for record/response. A TD F 15-05.10 shall be attached to any original documents

maintained on file. All recipients shall either sign the form or have their names annotated on the form. Recipient's signatures shall include the names of those who physically handled the document (professional, secretarial and/or office support staff) and those orally briefed on the substance of the information. This provides effective accountability and tracking of all individuals authorized access to the information.

- Maintain receipts of the transfer and destruction of Top Secret information for a full three years and receive appropriate follow-up reports from subordinate office/bureau TSCOs concerning their disposition of Top Secret documents. Using the follow-up reports, update the Top Secret Document Control Registry. The follow-up procedure maintains appropriate accountability records and ensures that no individual transmits Top Secret information to another individual or office without the knowledge and consent of the TSCO or alternate.

- Assign Top Secret document numbers to all incoming and newly created documents in a calendar-year sequence, e.g., TS 11-001 and TS 11-002. "TS" is the abbreviation for "Top Secret", 11 is the fiscal year when the document is initially recorded, and 001 and 002 are the first and second documents so recorded. The Top Secret document number shall be indicated on the face of the document in the upper right-hand corner. The same number shall be used for tracking purposes on the Top Secret Document Record and on any receipt.

- Verify recipients have a Top Secret security clearance, need-to-know, and storage capability before such information is released and/or assigned to appropriate staff for action/response.

6. DO/Bureaus and Security Point-of-Contact Responsibilities

a. DO/*Bureau Responsibilities.* DO/bureau office directors shall designate one or more security points-of-contact (SPC), depending on the size of their organization, as a liaison representative with in-house security officials. The designated SPCs shall receive training from DO/bureau security officials on handling classified information.

b. *Security Point-of-Contact's Responsibility.* Each SPC shall have a security clearance at the highest level of collateral information handled within that office. The responsibilities of the SPC include, but are not necessarily limited to, the following:

- Coordinating employees attending refresher/annual and specialized training.

- Serve as the primary office conduit for handling classified information.

- Responding to non-technical security inquiries from staff.
- Annually compiling statistical information on classification activity and security-related costs.
- Maintaining and stocking supplies of security forms.
- Internally disseminating security handout material (posters, notices, etc.).
- Alerting security officials about needed security container repairs.
- Reporting problems with security equipment (alarms, locks, shredders, etc.).
- Providing security officials information on suspicious persons, calls, packages, or activities.
- Advising employees how to report foreign contact information, as warranted.
- Requesting card access keys/cards/fobs, as applicable.
- Notifying security officials about classified waste collection, as needed.
- Requesting security awareness training.

Chapter III
Section 16

Destruction of Classified and Sensitive Information

Updated
6/17/11

1. Destruction Process

Classified information approved for destruction shall be completely destroyed to thwart retrieval and to prevent recognition and reconstruction. Approved destruction methods vary depending on the type of media used, e.g., for paper documents, burning, cross-cut shredding, wet-pulping, and pulverizing. For other classified media examples include: melting, degaussing, and chemical decomposition. The methods (and options) may be limited within a particular state, county, or municipal area. The type of destruction selected by Treasury/bureau components shall be appropriate to the local jurisdiction or area and might restrict the actual method that may be used.

a. *Destruction of Top Secret Information.* Top Secret information shall be destroyed in the presence of two cleared individuals; one person performs the actual destruction and the other person serves as a witness. Both individuals shall sign the *Classified Document Certificate of Destruction*, Treasury Department Form (TD F) 15-05.5. The completed TD F 15-05.5 shall be maintained on file for a three-year period after which it may be destroyed. No record of the destruction of the certificate is required.

b. *Destruction of Secret or Confidential Information.* Secret or Confidential information does not require a destruction certificate. Non-record classified information such as extra copies and duplicates, including hand-written notes, preliminary drafts, and other material of similar temporary nature, shall also be destroyed by burning, mulching or shredding as soon as its utility is expended. No records of such destruction are required.

c. *Destruction of Sensitive Information.* Sensitive information shall be destroyed in the same manner as Secret and Confidential.

2. Approved Destruction Equipment

The following are approved types of equipment for destroying hard-copy (paper) classified information and classified information on electronic/magnetic media:

a. *Cross-Cut Shredders.* Treasury/bureau destruction of classified paper media shall be performed using one of the high-security cross-cut shredders listed on the National Security Agency (NSA), Central Security Service (CSS) evaluated products list at http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml. Note that inclusion of a product on this list is not an endorsement by NSA, Treasury, or the U.S. Government. End users are encouraged to contact the shredder manufacturers

and distributors for help in selecting the equipment best suited to their individual requirements and to accommodate the anticipated volume of classified paper media to be destroyed.

Treasury/bureau users of cross-cut shredders are encouraged to dispose of the residue in several waste baskets, bins, or receptacles. The shredded paper should be distributed as such because the shredding process itself is not the final disposition. The shredded paper is still disposed of in some manner depending upon the location and the mode of waste removal that is used in each facility.

b. *Burn-bags for Temporary Storage*. Secret and Confidential information to be destroyed may be torn and placed in sealed opaque containers commonly designed as "burn-bags." Burn-bags appear with the words "burn" or "classified waste," or feature multiple alternating groupings of red and white diagonal stripes.

Use of burn-bags to store Top Secret information, pending final destruction at a later date, is not authorized.

Burn-bags awaiting destruction must be protected while in the end-users custody. The protection includes the user having a direct "line of sight" or "field of control" over the bags, depending on the office configuration. Burn-bags shall only be collected and contents destroyed by cleared contractor personnel or facilities maintenance personnel, and/or persons authorized by Treasury/bureau security officials.

When not in active use, burn-bags containing classified waste shall be protected commensurate with the level of classified contents and be secured at the close of business in a General Services Administration (GSA)-approved security container, (or until October 1, 2012 in a bar-lock cabinet). Burn-bags containing classified information may also be stored within a Sensitive Compartmented Information Facility (SCIF) or security-approved open storage area pending collection by authorized personnel. Burn-bags containing classified information that are located outside a SCIF or open-storage area must not be left unattended at any time.

c. *High-Security Disintegrators and Degaussers*. NSA produces a list of high-security disintegrators for disposing of paper/plastic/punched-tape material at http://www.nsa.gov/ia/_files/government/MDG/EPL-Degausser25February2010.pdf .

NSA also produces a list of degaussers for disposing of magnetic media. Specifications concerning appropriate equipment and standards for destruction of other storage media may be obtained from GSA.

d. *Electronic Media and Equipment.* Technical guidance on destruction (methods, equipment, and standards for disposing) of classified electronic media and processing equipment components may be obtained through Treasury's Office of Security Programs (OSP). Specifications concerning appropriate equipment and standards for destruction of other storage media may be obtained from GSA.

Chapter III Section 17

"Spill" Handling Procedures for Classified Information Found and/or Discovered on Unclassified IT Systems

Updated 10/21/11

1. Introduction

Treasury's local area network, also called the DO LAN and equivalent Bureau LANs are not approved for handling or processing classified information. Only the Treasury Foreign Intelligence Network (TFIN) and the Treasury Secure Data Network (TSDN) are approved information systems for classified word-processing. TFIN is approved for Top Secret/SCI information and TSDN is approved for Secret and Confidential.

The term "Spill" describes any circumstance involving classified information processed, communicated, transmitted, forwarded, or otherwise found to be contained on unclassified Departmental Offices (DO)/bureau information systems including when classified information is electronically processed or otherwise shared internally within or between DO/bureau components, as well as received from a non-Treasury/bureau external source on an unclassified information system and particularly via the Internet.

This section is the model for DO/bureaus to report, contain, and resolve any spill and procedural requirements apply equally to all persons initially discovering (and/or suspecting) classified information may have tainted an unclassified DO/bureau information system.

2. Reporting the Spill and its Content

a. *Contact Information.* DO/bureau information technology and security officials shall publish reporting components and corresponding phone numbers within their organization which are responsible for handling a reported spill. This includes contact numbers and email addresses during official working hours and non-duty hours.

b. *TD F 15-05.21, Report of Security Incident.* While initial notification of a spill may be via phone/email it shall be followed by completion of TD F 15-05.21 no later than the next business day and final notification when the spill has been cleansed from DO/bureau systems. Completed TD F 15-05.21 forms shall be made an official record of reported security incidents/spills including:

- The reporting and contact official(s) for further information by name and DO/bureau organization, email address, phone and fax numbers.
- Date/time spill occurred.
- Date/time reported to the Director, OSP.
- Type of security incident, e.g., cyber, physical/other.
- Unclassified description identifying known recipients.

- Estimated impact, e.g., high/moderate/low or none.
- Involvement of privacy information and number of affected persons.
- Identification of lost/stolen equipment and encryption.
- Reporting to law enforcement and/or OIG, TIGTA, SIGTARP.

To contain the spill, the classified information must not be forwarded by email or any other electronic means as it would further contaminate unclassified information systems and those work stations that received the spill must be protected to prevent further dissemination.

3. IT Officials' Responsibilities

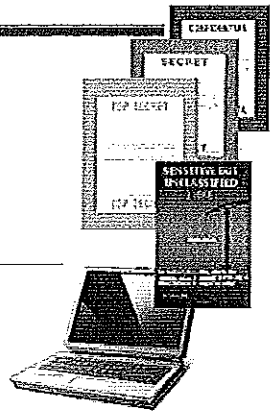
IT officials shall alert other DO/bureau recipients via e-mail of the initial spill with a high priority e-mail bearing a new subject line marked "**URGENT, URGENT, URGENT**" in bold, upper case, underlined text. This notice shall advise recipients it is important to contain the spill and the information must not be opened, deleted, saved (to their hard drive/disk) or forwarded.

Designated IT staff will take immediate action to sanitize the affected personal computers and information systems to further contain and clean up the spill. DO/bureau recipients of classified information on unclassified systems are expected to cooperate fully with IT staff charged with responsibility for the cleansing and with security officials handling such incidents. IT staff will advise their DO/bureau Chief Information Officer of progress in their system/equipment cleansing and in writing upon completion to the Department's CIO. IT officials shall keep statistical records of TD F 15-05.20 reports of what occurred, when and where, and which other DO/bureaus offices were affected by spills.

After cleansing is complete, the cognizant security official shall determine whether an investigating security official should be assigned to determine the circumstances surrounding the incident and take appropriate action that includes scheduling attendant training to keep employees, contractor personnel, consultants, detailees, etc., current on these procedures in the event of a future spill.

4. Bureau Security Officers' Responsibilities

Bureau security officers shall follow these procedural requirements in notifying their employees, contractor personnel, consultants, detailees, etc., how spills shall be reported, handled, and cleansed within their bureau. The procedural requirements include working with equivalent bureau IT staff and also reporting to the Director, Office of Security Programs about any spill, cleanup and investigative findings, conclusion(s), and actions taken.



Department of the Treasury

REPORT OF SECURITY INCIDENT - Date: _____

Reporting Official: _____ DO Office/Bureau: _____

Contact Official for further information: _____
(Federal Employee/Contractor)

E-mail Address: _____

Phone: _____ Fax Number: _____

Date/Time (include Time Zone) Security Incident Occurred: _____

Date/Time Reported to Treasury's Office of Security Programs: _____

Type of Security Incident: (check one) Cyber: ☐ Physical: ☐ Other: ☐ (specify below)

UNCLASSIFIED DESCRIPTION OF SECURITY INCIDENT: (describe briefly and include remedial efforts taken; use additional sheet if necessary)

Estimated Impact to DO Office/Bureau: High: ☐ Moderate: ☐ Low: ☐ None: ☐

Privacy Information Involved: Yes: ☐ No: ☐ Number individuals impacted: ____
If yes, describe types of Personally Identifiable Information (e.g., names, SSN, etc.)

Lost/Stolen Equipment: Name of System Impacted: _____ _____
(Encrypted) Yes: ☐ (include information about encryption) No: ☐ Unknown: ☐

Reported to Appropriate Law Enforcement? Yes: ☐ No: ☐
Reported to Treasury OIG/TIGTA or SIG/TARP? Yes: ☐ No: ☐

TD F 15-05.21

Chapter III
Section 18

Investigating the Loss, Possible Compromise, or Unauthorized Disclosure of Classified Information

Updated 6/17/11

1. Introduction

Departmental Offices (DO)/bureau employees, contractor personnel, or consultants knowledgeable of the loss or possible compromise of classified information shall immediately report the circumstances to DO/bureau security officials. Such officials shall then immediately notify the Director, Office of Security Programs (OSP), of the relevant facts, initial assessment and steps taken to contain and conduct a formal assessment of the damage.

2. Official Inquiry

Based on the circumstances, the Director, OSP shall either notify the Inspector General, the Inspector General for Tax Administration, the Special Inspector General for the Troubled Asset Relief Program or one or more DO/bureau components for additional investigation. At the conclusion of the official inquiry, the Director, OSP shall recommend administrative, disciplinary, or possible legal action based upon the jurisdictional authority of DO/bureau components involved and to ensure implementation of appropriate corrective actions.

The Director, OSP shall notify the Deputy Assistant Secretary for Security and the Assistant Secretary for Intelligence and Analysis whenever sensitive compartmented information is suspected or actually lost and/or subject to unauthorized disclosure.

3. Unofficial Publication or Disclosure

Unauthorized disclosures of classified documents (whether in the broadcast news or print media, on a blog, or on websites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by DO/bureau employees and contractors, until it is declassified by an appropriate U.S. Government authority.

DO/bureau employees and contractors have the following obligations with respect to the treatment of classified information and the use of non-classified government information technology systems:

a. Except as authorized by DO/bureau procedures, employees or contractors shall not, while using computers or other devices (such as Blackberries or

Smart Phones) that access the web on non-classified government systems, access documents that are marked classified (including classified documents publicly available on websites), as doing so risks that material still classified will be placed onto non-classified systems. This requirement applies to access that occurs either through DO/bureau or contractor computers, or through employees' or contractors' personally-owned computers that access non-classified government systems. This requirement does not restrict employee or contractor access to non-classified, publicly available news reports (and other non-classified material) that may in turn discuss classified material, as distinguished from access to underlying documents that themselves are marked classified (including if the underlying classified documents are available on public websites or otherwise in the public domain).

b. DO/bureau employees or contractors shall not access classified material unless a favorable determination of the person's eligibility for access has been made by personnel security officials, the person has signed an approved non-disclosure agreement, the person has a need to know the information, and the person has received contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

c. Classified information shall not be removed from official premises or disclosed without proper authorization.

d. DO/bureau employees and contractors who believe they may have inadvertently accessed or downloaded classified or sensitive information on computers that access the web via non-classified government systems, or without prior authorization, should contact their security and IT security offices for assistance.

4. Damage Assessments

Following an inadvertent or unauthorized disclosure or publication of information identical or similar to information that has been classified in accordance with EO 13526 or predecessor Orders, a determination shall be made of the degree of damage to the national security, the need for continued classification, and, in coordination with the DO/bureau organization or outside agency in which the disclosure occurred, what action(s) must be taken to prevent similar occurrences.

DO/bureau security officials shall establish a system of control/internal procedures to ensure that damage assessments are conducted in all cases involving the loss or possible compromise of classified information and to ensure that records are maintained in a manner facilitating retrieval, use, inspection and analysis.

DO/bureau components that were directly or indirectly responsible for the loss or possible compromise of classified information shall assist but not be responsible for conducting the official inquiry. This is to ensure the impartiality and fairness of the inquiry and the resulting damage assessment. Elements within the responsible office(s) or bureau(s), including subject-matter experts, shall cooperate with security officials and others assigned to the inquiry. They may suggest particular methodologies to be used as well as corrective actions, but may not lead the actual official inquiry.

Where the Director, OSP determines that a potential conflict might exist or the loss or unauthorized disclosure involves a senior DO/bureau official, the Deputy Secretary shall decide what DO/bureau entity shall be responsible for leading the inquiry. If the latter's office is involved, the deciding official shall be the Secretary of the Treasury.

5. Content of Damage Assessments

A damage assessment shall determine the potential and/or actual harm caused by the loss or unauthorized disclosure of classified information and the sensitivity, value, utility and source(s) thereof. All damage assessments shall be in writing, processed on equipment approved at the highest level of classified information contained therein and include the following:

- Identification of the complete facts, source(s), date(s) and circumstances of the compromise.
- Classification and description of the specifically lost/disclosed information.
- Analysis and statement of the known or probable damage to the national security that has resulted or that might be expected to result.
- Determination of the possible advantage to foreign powers resulting from the loss or compromise.
- Decision on whether the classification of the lost/compromised information should be continued without change, or if the specific information (or parts thereof) shall be modified to minimize or nullify the effects of the reported compromise and the classification retained, or if downgrading/declassification or upgrading is warranted, and if so, confirmation of prompt notice to known holders to alert them to any change.
- The scope of any significant loss or unauthorized disclosure, security violation or compromise.

- The significance to the national security.
- Contributing security deficiencies and evaluation of whether countermeasures are appropriate and feasible to negate or minimize the effect(s) of the compromise.

The final report shall be signed by the person(s) tasked with responsibility for the inquiry and include:

- The executive summary.
- Pertinent (and properly marked) information in a classified annex/addendum.
- Findings and other observations.
- Recommendations and follow-up action(s) to prevent recurrence.
- Actions taken to date, anticipated and assignment of specific tasking(s).

The Director, OSP, shall notify security counterparts in other departments or agencies which originated the information, and any other affected parties to enable them to conduct their own damage assessment and measures to negate or minimize any adverse impact caused by the loss or possible compromise.

6. Cases Involving more than One Agency

Whenever a loss or compromise involves the classified information or interests of more than one agency, the Director, OSP, shall immediately advise the other affected agencies of the circumstances and initial findings. Whenever a damage assessment will incorporate the product of two or more agencies the affected agencies shall agree upon the assignment of responsibility for the assessment. DO/bureau components will provide all data pertinent to the compromise to the agreed-upon agency to enable it to conduct the damage assessment.

When a loss or compromise of U.S. classified information is the result of actions taken for foreign nationals, or by foreign government officials, or by U.S. citizens in the employ of international organizations, the agency performing the damage assessment shall endeavor to ensure, via intergovernmental channels, that information pertinent to the assessment is obtained. If more than one agency is responsible for the assessment, they shall coordinate the request for information via appropriate intergovernmental channels. Foreign governments (including those allied with the U.S. Government) will not normally be advised of any security system vulnerabilities that contributed to the compromise.

Whenever a formal action, beyond a reprimand, is contemplated against any person believed responsible for the loss or compromise of classified information, damage assessments shall be coordinated with proper legal counsel. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, coordination shall be made with the Department of Justice (DOJ) and the DO/bureau legal counsel where the individual is assigned or employed.

The designated representative of the Office of the Director of National Intelligence (ODNI), or other appropriate intelligence community official responsible for the information involved, shall be consulted by the Assistant Secretary for Intelligence and Analysis or his/her designee whenever a loss or compromise of sensitive compartmented information has occurred.

7. Notification to the Information Security Oversight Office (ISOO)

The Senior Agency Official shall notify the Director, ISOO when officers and DO/bureau officials, employees, contractor personnel, licensees, certificate holders and/or grantees are subject to appropriate sanctions if they knowingly, willfully, or negligently disclosed to unauthorized persons information properly classified under E.O. 13526 or predecessor orders; classify or continue the classification of information in violation of E.O. 13526 or any implementing directive; or create or continue a special access program contrary to the requirements of E.O. 13526 and that is:

- Reported to oversight committee in the Legislative branch.
- May attract significant public attention.
- Involves large amounts of classified information;
- Reveals a potential systemic weakness in classification, safeguarding or declassification policy or practices.

Chapter III **Handling Security Infractions, Investigating** Updated
Section 19 **and Adjudicating Security Violations** 5/16/14

1. Safeguarding Responsibility

This section establishes procedures for investigating and adjudicating reported security infractions and security violations. Primary responsibility for safeguarding classified information from possible loss, compromise or unauthorized disclosure rests with each person possessing a security clearance. Every cleared person having knowledge and physical custody of, or access to, classified information also has this responsibility. Classified information shall be properly protected at all times. The failure to do so might constitute a security infraction/violation depending on the circumstances and/or the possibility of ensuing compromise, loss, or access to classified information by unauthorized persons.

2. Security Infractions

Security infractions are incidents involving a deviation from governing security regulations that does not result in an unauthorized disclosure, loss or compromise of classified information but which increases the probability of an actual security violation. Examples might include but are not necessarily limited to the non-use of security forms for safeguarding/accounting for classified information - such as document cover sheets, records of safe combinations, security container forms, OPEN/CLOSED signs, or not checking classified work areas before close of business and/or improperly assuming someone else will protect classified information.

3. Security Violations

Security violations are any knowing, willful, or negligent action; (1) that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) to classify or continue the classification of information contrary to the requirements of Executive Order (E.O.) 13526, or its implementing directives; or, (3) to create or continue a special access program contrary to the requirements of E.O. 13526.

Repeated abuse of the classification process, either by unnecessary or over-classification, or repeated failure, neglect or disregard of established requirements for safeguarding classified information shall be grounds for appropriate adverse or disciplinary action. Such actions may include, but are not limited to, verbal counseling/warning, letter and warning, letter and reprimand, suspension without pay, reassignment, and revocation of security clearance, demotion or dismissal.

Types of Security Violations. Examples of security violations include, but are necessarily Limited to, the following actions involving classified information:

- Improper:
  - Transmission (mailing, hand-carrying, e-mailing).
  - Storage.
  - Packaging.
  - Reproduction.
  - Processing on non-approved IT systems/equipment.
  - Marking.
  - Destruction.
- Failure to:
  - Secure classified documents.
  - Apply all required markings on classified documents.
  - Lock security container/bar-lock cabinet or equipment.
  - Protect burn bags containing classified waste prior to destruction.
  - Safeguard classified communications security (COMSEC) information.
  - Verify security clearance of recipients prior to sharing classified information.
  - Verify need-to-know and/or need-for access to classified information.
  - Report the loss or possible compromise of classified information.

4. Responsibility for Reporting Security Violations

Cleared employees and contractor personnel are required to report any suspected security violation to Departmental Offices (DO)/bureau security officials. Individuals who report security violations may do so via phone, email or in person. The reporting individual should ensure that classified information is not included in their report. DO/bureau security officials shall notify the Director, Office of Security Programs (OSP) of any alleged security violation, in writing (including via e-mail), within 24 hours of initial discovery.

5. Reporting Security Violations to the Inspectors General and Reports to the Information Security Oversight Office (ISOO)

All reports of valid security violations received by the Director, OSP (including those regarding classified information or collateral national security systems) shall be brought to the attention of the Treasury Inspector General for Tax Administration (TIGTA), if the report is from the Internal Revenue Service (IRS), IRS-Criminal Investigations, IRS

Office of Chief Counsel, or the IRS Oversight Board, to the Special IG for the Troubled Asset Relief Program (SIGTARP), if the report involves TARP, or to the Treasury Inspector General (OIG) if from any other DO/bureau component within the Department. The Director, OSP is responsible for investigations of alleged violations unless the OIG or TIGTA or SIGTARP advises, in writing, that they wish to conduct such investigation.

When the Director, OSP determines a security violation has resulted in properly classified information being disclosed to unauthorized persons; or information has been classified (or continues to be classified) in violation of the EO and/or ISOO Directive; a special access program has been created or continued in violation of the EO and/or ISOO Directive; or any other provision of the EO and/or ISOO Directive has been contravened, that official shall so notify the Director, ISOO and provide a report to the Senior Agency Official ensuring corrective steps are taken. The Director, OSP shall also report to the Director, ISOO when there are confirmed instances of the occurrence of declassification without proper authority.

6. Investigating Reported Security Violations

When it is determined that an inquiry of an alleged security violation is warranted and that OSP shall conduct it, the Director, OSP shall select and assign in writing a responsible and appropriately cleared security official to conduct the inquiry.

The Director, OSP shall ensure the official conducting the inquiry has DO/bureau credentials to substantiate his or her authority to others during the course of the inquiry. The official shall examine circumstances surrounding the alleged violation, which may include reviewing documentation, inspecting office space and work areas, interviewing DO/bureau employees and contractor personnel, and taking statements as warranted. The assigned official shall collect information and put it into format noting background information; findings of fact; conclusions; and, recommendations. Statements and other information which support findings of facts shall be included in the assigned official's report to the Director, OSP who will make a determination as to whether a violation occurred and who was responsible. The Director, OSP may require further inquiry before making his or her determination.

The Director, OSP is responsible for recommending, in writing, individual disciplinary actions to the supervisor of the responsible person(s). The Director, OSP shall notify the responsible contracting officer if contractor personnel appear to be responsible for a security violation. Similar notice shall be sent to security officials of any detailees from other Treasury bureaus or other agencies. In addition, the Director, OSP shall determine the need for specific and enhanced training and provide recommendations to the affected DO/bureau component for procedural modifications to prevent possible recurrences.

The DO/bureau employee's supervisor shall also be notified in writing by the Director, OSP of the determination as to whether the employee is responsible for a security violation. The employee will be notified in writing of any proposed disciplinary action by his or her supervisor. Supervisors are responsible for providing OSP a copy of any

supervisory disciplinary action(s) taken with respect to an employee responsible for a security violation. Such documentation along with the inquiry and other pertinent information will be filed in the individual's security folder for a period of three years. Where supervisors do not take disciplinary action or provide documentation thereof, OSP's records shall reflect this and the Director, OSP shall so notify the Deputy Assistant Secretary for Security. Bureau security officers shall keep like records with respect to security violations within their organization and so notify the Director, OSP.

7. Authorized Security Inspections, Security Officials, and Actions

Credentialed DO/bureau security officials or other designated persons with an appropriate security clearance are authorized to conduct inspections before, during and after official business hours as approved by the Director, OSP. In performance of their official duties, security officials are authorized to enter offices and view the tops of desks, the inside of already-opened drawers/cabinets/security containers, and other miscellaneous office furniture and equipment in plain view in any DO/bureau-owned or -leased buildings or offices. Security inspections are intended to ensure that the requirements of E.O. 13526, Treasury's Security Manual (TD P 15-71), and applicable DO/bureau regulations for safeguarding classified information are properly executed and that classified information is provided the required level of protection.

Officials conducting security inspections are authorized to enter randomly designated offices except a Sensitive Compartmented Information Facility (SCIF). Access to any SCIF must be coordinated with Treasury's Senior Official of the Intelligence Community (SOIC) in the Office of the Assistant Secretary for Intelligence and Analysis who is responsible for controlling/operating DO/bureau-operated SCIFs.

8 Record of Security Violation (RSV) Form

Whenever an apparent security violation has been discovered, inspecting security official(s) shall complete a Treasury Department Form (TD F) 15-05.6, *Record of Security Violation* and forward it to the appropriate DO/bureau security office. Employees suspected of being involved in a security violation shall be notified thereof via the RSV. The form is the baseline for reporting that an individual's action or lack thereof (whether knowingly, willfully or through negligence) is in violation of E.O. 13526, and/or other applicable DO/bureau regulation. The form is located on-line at http://thegreen.treas.gov/policies/Forms1/Record%20of%20Security%20Violation.pdf.

a. *Completing the RSV Form.* The official who discovered the security violation will complete Part I of the RSV form and indicate the date, time, and highest level of classified information involved. This official will also include a brief description of what was found, where it was found, and any other relevant information. The RSV form should not contain any classified information. However, if classified information is pertinent, it shall be contained in a separate, appropriately marked, transmitted, and safeguarded memo to the Director, OSP.

Bureau RSV forms shall be directed to and handled by the bureau security officer or equivalent position.

Upon completion of a preliminary inquiry by the DO/bureau security official, the RSV form and any related information shall be forwarded to the person allegedly responsible for the security violation for their completion of Part II. That person shall sign Part II (where indicated) and is encouraged (but not required) to indicate their knowledge of what occurred. The person's supervisor shall complete and sign Part III. Completed RSV forms shall be returned to the DO/bureau security official for adjudication.

9. Adjudicating Reported Security Violations

a. *Adjudicating Domestically Reported Security Violations*. The Director, OSP shall maintain records pertaining to all reported security violations pending final adjudication. If it is determined that the alleged security violation is unfounded, the documentation relating to the reported incident shall be noted as such and no further action will be taken.

In the event of a determination that a security violation is substantiated, written notification shall be provided to the responsible individual(s) by his or her supervisor. The supervisor shall consider the recommendation of the Director, OSP. The recommendation shall be based on, among other things, the nature of the security violation, the frequency and seriousness of any earlier violations (within the last 2 years), and the administrative disciplinary guidelines in paragraph 10 below and ensure consistency in attendant recommendation(s) for possible disciplinary action. The supervisor must be able to justify why they do not accept the Director, OSP's recommendation with respect to disciplinary action of a valid security violation.

A copy of all documentation relating to the security violation shall be filed in the security violation indices of the DO/bureau security officer and in the individual's personnel security file. DO/bureau security officers shall advise the Director, OSP in writing within five business days of any action taken regarding such security violations.

Adjudicating Overseas Reported Security Violations. Alleged security violations committed by DO/bureau employees assigned or traveling through overseas posts, are reported by the Department of State (DOS) to the Director, OSP. State's preliminary inquiry includes an assessment of possible compromise. When the Director, OSP receives State's RSV form, the individual responsible and the post or unit security officer usually will have provided information about the reported violation with or without related comments. In the event sufficient background information is lacking, the Director, OSP may request supplementary details to assist in the adjudication process. The Director, OSP shall review and evaluate the information concerning the alleged security violation and forward State's RSV

form to the DO/bureau component for processing

10. Administrative Disciplinary Guidelines

a. After establishing the responsibility for a security violation, the Director, OSP or the bureau security officer shall initiate administrative action by making a recommendation to the responsible person's supervisor for disciplinary action. Disciplinary action will be taken in accordance with the guidelines set forth below.

Violation	*Possible/Available Disciplinary Action*
First Security Violation	Verbal counseling/warning → written reprimand → removal
Second Security Violation	Written reprimand → removal
Third and Subsequent Security Violation	Written reprimand → removal

b. In conjunction with notice to the supervisor of a person found responsible for a security violation, the Director, OSP (or bureau security officer) shall also notify the responsible person. The notice shall contain the following statement: "You have the right to appeal this determination to the Department of the Treasury's Deputy Assistant Secretary (DAS) for Security within ten business days of your receipt of this notice." The appeal should be addressed to:

Security Violation Appeals
c/o Director, Office of Security Programs
Room 3185 Treasury Annex
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20220

The Director, OSP will notify the DAS, Security of receipt of all appeals for the latter's review. The appeal must be in writing and contain the following information: (1) employee's full name, address and telephone number(s); (2) a copy of the Director, OSP or bureau security officer's employee notification; and, (3) any written statement, relevant documents, materials, or information that the employee wishes the DAS, Security to consider.

c. An appeal filed outside the ten business day limit will not be accepted by the DAS, Security unless the employee demonstrates good cause for the delay. The failure of the employee to request an appeal within the required time limit will result in a termination of any further appellate proceedings.

d. If the DAS, Security determines that additional information or clarification is necessary to render a decision, he or she will request such information from the DO/bureau where the case originated. The respective DO/bureau component shall ensure that the request is fulfilled in a timely manner. There is no

administrative appeal of a decision by the DAS, Security regarding a security violation.

11. Relationship to Other Procedures

The appeal of a security violation determination may be decided without regard to other procedures that may be invoked by the person charged with responsibility for the violation, including a grievance, an appeal to the Merit Systems Protection Board, a complaint filed pursuant to Equal Employment Opportunity Commission (EEOC) regulations, a complaint to the Office of Special Counsel or any security clearance determination. Information obtained during the appeal of a security violation determination may be relevant to other proceedings. The Director, OSP shall assess requests for information or action before making a disclosure of information or taking other action regarding the security violation appeal. Depending on the severity of a particular security violation, the Director, OSP may elect to temporarily suspend an employee's access to classified information following the procedures in Chapter I, Section 6.

Chapter III
Section 20

Classification Challenges

Updated
6/26/13

1. Introduction

Information classified under Executive Order (E.O.) 13526 and prior Orders is subject to challenge by any authorized recipient of the information. This section establishes Department of the Treasury procedures for exercising such challenges in addition to handling allegations or complaints regarding over-classification or incorrect classification.

2. Authorized Holders May Challenge Classifications

An authorized holder of information who in good faith believes the classified status of particular information is improper is encouraged *and expected* to challenge the classification status of the information.

An authorized holder is any individual, including an individual external to the Departmental Offices (DO)/bureaus having: (1) undergone a favorable determination of eligibility for access to classified information; (2) signed an approved non-disclosure agreement; (3) has a need-to-know the information and (4) received training as required by E.O. 13526. Only the following personnel qualify as authorized holders for purposes of making a challenge:

- Cleared U.S. Government employee who is a recipient of the particular classified information in the course of conducting official business.
- DO/bureau security officer who is responsible for properly safeguarding classified information.
- Cleared contractor personnel or consultant who is performing work or providing services involving access to classified information.

3. Reasons to Challenge Classification Decisions

Challenges of classification decisions are intended to bring about corrective action(s) that ensures only information legitimately warranting protection based upon criteria in E.O. 13526 is classified. The decision to challenge shall be based on one of the following assumptions:

- Information should/should not be classified.

- Information should be classified at a lower/higher level (under/over-classification).
- Information is improperly classified (including an overly restrictive period of time or without proper authority).
- Information is improperly marked.

Challenges highlight and serve as a deterrent factor in careless or improper classification decisions. While the potential exists that frivolous challenges might be initiated, the intent is to improve credibility, internal oversight, and reduce excessive classification. Having been authorized access to classified information it is the responsibility of all cleared employees to ensure such information is adequately safeguarded. This task includes noting and reporting to appropriate classifiers any conditions that lead an employee, contractor personnel, or consultant to feel the actual classification or exercise thereof is improper, needless, or restrictive.

4. Allegations and Complaints regarding Over-classification or Incorrect Classification

Where an authorized recipient of classified information feels, in good faith, that particular information is improperly classified but not challenged under that provision of the EO, the subject documentation shall be preliminarily marked (if not already) with the recipient's recommended level of classification and protected at that level pending a final decision by appropriate DO/bureau authority. Any electronic discussions incident to the allegation or complaint shall take place over the Treasury Secure Data Network (TSDN) at the Secret classification level. If the recipient exercises the challenge provision of the EO the documentation in question shall be further handled under the procedures described in this Section. Further guidance on proper classification markings is contained in Chapter III, Section 5.

5. Preventing Adverse Actions, Non-Retribution and Protecting Whistleblowers with Access to Classified Information

A classification challenge shall not be cause for improper treatment of employees, contractor personnel, or consultants, or adverse action being initiated, considered, or taken by supervisors (or higher-level officials) in evaluating and rating employee performance. Similarly, challenges shall not be considered in making decisions on the on-time fulfillment of contractual obligations of contractor personnel or consultants who have been authorized access to classified information. Those who exercise a classification challenge will not be subjected to adverse action, reprisal, retribution, or retaliation based on their election to engage the challenge provision.

General employee protections from retribution are addressed in 5 United States Code (USC) §2302, specifically sections (b)(8) and (b)(9); Treasury Order (TO) 102-08, *Authority to Take Final Action with Respect to Prohibited Personnel Practices*, dated November 5, 1986; Transmittal No. 99-01, *Whistleblower Protection Act*, dated May 5, 1999 and Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information,* dated October 10, 2012. The latter ensures that employees who are eligible for access to classified information, can effectively report waste, fraud, and abuse while protecting classified national security information and prohibits retaliation against employees for reporting such waste, fraud and abuse. (See Chapter I, Section 8).

6. Description of Challenge Requirement and Handling

Challenges to classification decisions shall sufficiently describe the particular information being challenged to enable the classifier (or his or her designee) to locate it and respond with a reasonable amount of effort. Authorized holders shall also identify their rationale behind the challenge (under/over-classification, improper markings, etc.). Throughout each challenge, holders of the information (together with all copies, drafts, reproductions, extracts, work sheets, etc.) must ensure that the material in question is suitably protected to prevent unauthorized access commensurate with the level of classification initially assigned to the information. In the case of any material that a challenger believes should be classified (but has not been), the information shall be protected at a level deemed appropriate pending the final DO/bureau decision.

The original and any copies of the "questionable information" shall be protected during the entire challenge in the same manner as other Top Secret, Secret, or Confidential information. This includes markings, packaging, transmittal, accountability, couriering, reproduction, etc., until such time as a decision is made. Where a challenge has been made to the same information within the past two years, or the subject is in pending litigation, the new challenge need not be processed beyond informing the challenger of this fact and of their appeal rights, if any. Classification challenges shall be considered separately from Freedom of Information Act (FOIA) or other requests and not processed in turn with pending FOIA or other access requests.

7. Informal Inquiry

Initial attempts shall be made to query the classifier informally if the authorized holder's question(s) may be resolved quickly. Such inquiries may be conducted by phone, fax, email (via the DO/bureau local area network), or in person, as long as the "questionable information" is protected. Use of the Treasury Secure Data Network (TSDN) is authorized provided both parties have accounts on that information processing system and the inquiry is kept to the Secret or Confidential level. If the inquiry resolves the challenger's questions, no further action is needed except to ensure the markings are appropriate for the particular information in question and other authorized recipients are so notified of any resulting changes.

8. Formal Challenges

If an authorized holder believes the informal response was insufficient, that it might involve more time, or be particularly complex to resolve, a formal challenge might be warranted. The formal challenge must be in writing but need not be more specific than to question why information is, or is not classified, or if it is classified at the appropriate level and/or for the proper time frame. The actual correspondence should be unclassified. Inquiries may also be made via the TSDN but must be kept to the Secret or Confidential level only. The DO/bureau LAN shall not be used for exercising a formal challenge to avoid contamination of classified information on an unclassified information system.

Each aspect of the authorized holder's inquiry shall be addressed depending on the nature of the challenge, such as: (1) whether the information should or should not be classified; (2) if it is over/under classified; (3) protected for an appropriate time frame and/or classified by the appropriately authorized official; or, (4) improperly marked.

DO/bureaus are responsible for promptly handing all classification challenges within the allotted time. The challenge shall be formally addressed to the DO/bureau official who initially made the classification decision if that official is still employed in the same capacity, and if not, to his or her successor. The DO/bureau official shall render a decision within 30 days of receipt and notify both the challenger and the Director, Office of Security Programs (OSP), in writing, of his/her decision and accompanying rationale. Where it is unclear or unknown who should render a decision on a challenge, the question shall be addressed to the Director, OSP, to determine which DO/bureau official(s) listed in TO 105-19, *Delegation of Original Classification Authority; Requirements for Declassification and Downgrading*, has subject-matter interest and jurisdiction over the particular information. The 30-day time-frame commences when the deciding DO/bureau official receives the formal challenge.

9. Impartial Review Official or Panel

At the discretion of the Director, OSP, an impartial official or panel of subject-matter experts may be asked to review the decision(s) by the classifier and to overrule or sustain that decision. The Director, OSP, shall serve as an advisor from a classification management and security perspective on the impending DO/bureau classification challenge.

10. Decision by the Deputy Assistant Secretary for Security or by the Senior Agency Official

When the initial classified information was created or generated by a DO/bureau official listed in TO 105-19, the challenge shall still be addressed to the Director, OSP. The originating DO/bureau official shall provide his/her input in response to each aspect of the classification challenge. As warranted, an impartial panel may be established to be

chaired by the Director, OSP.

However, the deciding official shall be either the Deputy Assistant Secretary (DAS) for Security, the Senior Agency Official (SAO), or the Acting SAO. The Director, OSP, shall refer the challenge with related documentation from the initial classifier to enable the DAS for Security, or the SAO or the Acting SAO, to make a final determination. Such determination shall be made, in writing, within 15 days of receipt.

Once the final determination has been made, the document or information will be annotated in conformance with standard identification and marking provisions of E.O. 13526. The challenge provisions of this section do not apply to, or affect, declassification review actions under the mandatory declassification review requirements of the Order.

11. Timeframes for Adjudication and Appeals

DO/bureaus shall provide an initial written response to a challenge within 60 days. If unable to respond to the challenge within that timeframe, DO/bureaus must acknowledge the challenge in writing and provide a date by which they will respond. The acknowledgment must include a statement that if no DO/bureau response is received within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel for a decision. The challenger may also forward the challenge to the Panel if DO/bureaus have not responded to an internal appeal within 90 days of their receipt of the appeal.

12. Notification to Challengers

Challengers shall be notified of the final DO/bureau decision in writing. This includes any change(s) made as a result of the challenge or the reason(s) why no change was made. The challenger shall also be advised in writing of his/her right to appeal DO/bureau decisions to the Interagency Security Classification Appeals Panel (ISCAP) established under EO 13526; decisions by the ISCAP are final. Such written decisions shall also be kept unclassified.

The Director, Information Security Oversight Office shall be notified by the Director, OSP, of any willful and knowing instances of improper classification, following a challenge, and advised of the decision.

Numerical statistics on challenges shall be reported annually by DO/bureaus on the Standard Form (SF) 311, *Agency Security Classification Management Program Data*, to the Director, OSP. Completed SF311s are due to OSP by October 15th every year.

Chapter III
Section 21

Self-Inspection Program for Classified Information

Updated
6/17/11

1. Self-Inspection

Self-inspection is the internal program review, evaluation, and assessment of individual Departmental Offices (DO)/bureau classification activities and the Department of the Treasury organization as a whole. This is a key element of evaluating employee comprehension of information security program requirements under Executive Order (E.O.) 13526, Information Security Oversight Office (ISOO) directives, the Treasury Security Manual (TD P 15-71), and applicable bureau issuances.

2. Process

a. DO/bureau offices shall establish and maintain an on-going self-inspection program that includes periodic review and assessment of their (original and derivative) classified products. The review and assessment includes DO/bureau components that receipt for classified information from other internal DO/bureau or external (non-Treasury) sources, but do not otherwise generate classified information. In such instances the self-inspection program might be limited to assessing individual employee awareness of regulations for safeguarding classified information and security practices or procedures in the relatively few components authorized access.

b. DO/bureaus shall designate appropriately cleared personnel to assist in carrying out periodic self-inspection programs. Those persons, including cleared contractor personnel, conducting self-inspections are also authorized to correct misclassification actions Individual DO/bureaus components shall determine the means and methodology for conducting self-inspections. Examples include, but are not necessarily limited to:

- Reviewing relevant security directives, guidelines and instructions for currency and applicability.
- Interviewing producers/processors and users of classified information to confirm understanding of information security principles and procedures.
- Reviewing access and control records and procedures (including Top Secret document registry logs) and actual holdings to verify adherence to dissemination, storage, accountability, transmission, and destruction requirements.

- Sampling actual classified (original and derivative) documents generated by DO/bureau activities, including electronically processed information, to ensure proper classification, marking, downgrading, and declassification actions are being followed.

- Assessing the effectiveness, employee understanding, and practical application of classification guides to properly create derivatively classified products.

- Evaluating, and as needed, modifying employee training.

3. Frequency of Self-Inspections

DO/bureau components generating classified information shall conduct at least one self-inspection annually that includes document reviews. To ensure DO/bureau employees remain current, the Office of Security Programs (OSP) may task particular organizations with conducting self-inspections to evaluate the knowledge base of assigned employees with respect to security requirements for protecting classified information, e.g., identifying classified information and document handling, storage, processing, accountability, packaging, transmission, reproduction, and destruction requirements.

4. Reporting Results of Self-Inspections

DO/bureau components will report the numbers of in-house inspections annually on Standard Form (SF) 311, *Agency Security Classification Management Program Data*, available at http://intranet.treas.gov/security/forms/ to the Director, OSP for inclusion in an overall Treasury Department annual report to the ISOO. The reporting components shall document their findings and attendant recommendations for improvement or enhancement. Findings should indicate that all reviewed records, documents, briefings, and activities were found to be in compliance with E.O. 13526 and applicable implementing directives or otherwise identify noted discrepancies and indicate where corrective action will be or has been taken. The results of individual self-inspections shall be analyzed to determine where greater coordination and security efforts should be exercised to ensure full compliance with protective requirements for marking safeguarding classified information.

5. Reporting Follow-up Actions

DO/bureau components shall conduct and document follow-up actions taken where individual self-inspections have identified such a particular need. This should also be the focus of subsequent training activity for affected employees. DO/bureaus shall document the findings of self-inspections internally and copies of such follow-up actions as may be necessary shall be provided to the Director, OSP.

Chapter III
Section 22

Critical Element for Security in Performance Evaluations

Updated
6/17/11

1. Introduction

The management of classified information is a critical element in evaluating the performance contract or other system used to rate personnel responsible for safeguarding classified information. Executive Order (E.O.) 13526 mandates the establishment and maintenance of security education and training for all persons who have a security clearance for access to classified information.

The requirement to annually include a critical element for security in individual performance evaluations supports the Secretary of the Treasury's commitment to heighten the importance of protecting classified information, information systems and equipment, and emphasizes individual responsibility. The use of a standardized element is intended to provide fair and consistent treatment of managers, supervisors, and management officials who have common duties and working conditions throughout the Departmental Offices (DO)/bureaus. DO/bureau Human Resources (HR) officers and security officers shall note this requirement and receive guidance for implementation from the Office of Human Resources Strategy and Solutions and the Director, Office of Security Programs (OSP).

2. Who Is Evaluated?

a. *Job Functions*. The following employees will be evaluated:

- Original Classification Authorities (OCA).
- Senior Executive Service (SES).
- Security managers and security specialists.
- All other personnel whose duties involve significant creation, generation or handling/processing classified information.

For DO/bureau purposes, the term "significant" implies more than an employee having a security clearance and who rarely works with classified information. The term entails an employee having regular, hands-on work with classified information in any type of capacity.

b. *Examples of Duties*. Examples of duties that would be deemed significant include, but are not necessarily limited to:

- Processing information on the Treasury Secure Data Network (TSDN) and Treasury Foreign Intelligence Network (TFIN).
- Proof-reading internal and/or out-going classified documents.
- Reading incoming classified material (including other agencies' information).
- Compiling statistical data on classification and security-related reports.
- Using security equipment and related security forms that involve protecting classified information.
- Verifying security clearances and need-to-know; conducting classified security training sessions.
- Preparing draft/final classified position-papers including those in electronic format.
- Using burn-bags for destroying classified documents.
- Reviewing and/or responding to Freedom of Information/Privacy Act requests involving classified records.
- Packaging, transmitting (by mail or electronically), hand-carrying classified documents within and between Treasury/bureaus.
- Accounting for the volume of classified documents.
- Serving as a Top Secret Control Officer and/or a Security Point of Contact official.
- Copying classified information.
- Attending classified meetings including taking official minutes.
- Safeguarding classified information.
- Researching and filing classified information.
- Marking classified documents.
- Destroying classified information.

DO/bureau employees engaged in any one of the above activities are deemed to have significant responsibility in the context of E.O. 13526.

c. *Suggested Performance Evaluation Criteria.* Sample performance evaluation criteria for rating individual employee's critical element for security performance evaluations as contained in paragraph 4 and categorized by the work normally performed by GS-0080-Security Series employees and similar responsibilities of emergency preparedness employees working with classified information. Citation of particular information in Attachment 1 is for illustration purposes and may be modified by DO/bureau supervisors to fit specific jobs that are performed.

3. Supervisor's Evaluation Responsibility

Supervisors shall discuss with affected employees examples of performance that will allow them to meet the critical element; circumstances that might result in a determination that the employee does not meet the critical element; and the potential impact of not meeting the element. Information contained in performance evaluations may be disclosed to DO/bureau officials who have a need for reviewing performance evaluation records in the course of their official duties.

4. Performance Evaluation Criteria

a. Original and Derivative Classifiers

- Exercises classification authority based upon criteria in E.O. 13526 as rationale warrant.
- Ensures proper classification, marking, and record-keeping of classified documents.
- Encourages challenges to classification actions that appear to be incorrect.
- Ensures subordinates have the need-to-know classified information and appropriate security clearance.
- Encourages training for subordinate staff and demonstrates attention to safeguarding requirements to protect classified information.
- Reports apparent or suspected attempts to access classified information by unauthorized persons and assists in official inquiries.

b.. Senior Executive Service

- Serves as the security role model setting an example within the organization.
- Fosters a culture of security awareness and high sense of responsibility for protecting classified information.
- When applicable, ensures all classified memos, emails, and other documents are processed on approved IT classified systems and properly marked.
- If classified information is inadvertently disclosed, takes immediate corrective measures.
- Reports to DO/bureau security officials any apparent or suspected attempt to access information by unauthorized persons and assists in official inquiries.
- Solicits training (including both annual and mandatory) for self and his/her organization on proper safeguarding requirements for classified information.
- As warranted, initiates requests for security clearances based on staff need for access to classified information and ensures employees complete required background investigation forms in a timely manner.
- Ensures subordinates whose duties significantly involve creation or handling of classified information are evaluated with respect to management of classified information in their own individual performance evaluations.

c. Information Security Specialist

- Updates and tailors training to needs of classifiers (and staff) on requirements for classifying and safeguarding classified information.
- Identifies and analyzes patterns of misunderstanding with respect to classification management requirements by staff and provides corrective action.
- Reduces instances of improper marking of classified documents.
- Reduces instances of security violations.
- Exercises challenges to classification actions that appear to be incorrect.
- Ensures records are maintained on all use of classification authority.
- Ensures originally/derivatively classified documents are properly marked.
- Monitors self-inspection reviews and inventories of classified documents to ensure proper classification, handling, accountability, safeguarding, and destruction.
- Checks security containers storing classified information.
- Acts on requests for assistance and reported problems with security equipment for protecting classified information.
- Compiles annual statistical information on volume of classified documents and security-related costs.
- Follows through on employee reports of attempts to obtain unauthorized access to classified information by un-cleared persons.
- Responds to classification management questions/inquiries.

d. Senior Operational Security Specialist or Equivalent

- Updates and tailors training to needs of classifiers (and staff) on requirements for classifying and safeguarding classified information.
- Identifies and analyzes patterns of misunderstanding with respect to classification management requirements and provides corrective action.
- Reduces instances of improper marking of classified documents.
- Reduces instances of security violations.
- Ensures records are maintained on all use of classification authority.
- Conducts self-inspection reviews and inventories of classified documents to ensure proper classification, handling, accountability, safeguarding, and destruction.
- Ensures originally/derivatively classified documents are properly marked.
- Checks security containers storing classified information.
- Acts on requests for assistance and reported problems with security equipment for protecting classified information.
- Follows through on employee reports of attempts to obtain unauthorized access to classified information by un-cleared persons.
- Responds to classification management questions/inquiries.
- Verifies clearances of persons requesting access to classified information.

- Ensures classified information is not provided to unauthorized persons.
- Reports any apparent or suspected attempt to access classified information by unauthorized persons and assists in official inquiries.

e. Operational Security Specialist or Equivalent

- Identifies and analyzes patterns of misunderstanding with respect to classification management requirements by staff and provides corrective action.
- Reduces instances of security violations.
- Conducts self-inspection reviews and inventories of classified documents to ensure proper handling, safeguarding, and destruction.
- Checks security containers storing classified information.
- Acts on requests for assistance and reported problems with security equipment for protecting classified information.
- Follows through on employee reports of attempts to obtain unauthorized access to classified information by un-cleared persons.
- Properly uses and maintains stock of standard forms to protect classified information.
- Attends training and keeps current on handling requirements for classified information.
- Verifies clearances of persons requesting access to classified information.
- Ensures classified information is not provided to unauthorized persons.
- Reports any apparent or suspected attempt to access classified information by unauthorized persons and assists in official inquiries.

f. Senior Security Specialist

- Attends training on and maintains understanding of safeguarding requirements for classified information.
- Serves as point of contact for security equipment for protecting classified information.
- Properly uses standard forms to protect classified information.
- Monitors destruction programs for classified information.
- Verifies clearances of persons requesting access to classified information.
- Ensures classified information is not provided to unauthorized persons.
- Reports any apparent or suspected attempt to access classified information by unauthorized persons and assists in official inquiries.

g. Senior Program Analyst

- Attends training on and maintains understanding of safeguarding requirements for classified information.
- Ensures classified documents are properly marked.
- Ensures that official contacts have the need-to-know classified information and appropriate security clearance.

- Properly uses standard forms to protect classified information.
- Verifies clearances of persons requesting access to classified information.
- Ensures classified information is not provided to unauthorized persons.
- Reports any apparent or suspected attempt to access classified information by unauthorized persons and assists in official inquiries.

h. Industrial Security Specialist

- Ensures contracting/project officers and security personnel are providing proper security classification guidance on industrial security contracts.
- Updates and tailors training to needs of classifiers (and staff) on requirements for classifying and safeguarding classified information.
- Identifies and analyzes patterns of misunderstanding with respect to classification management requirements and provides corrective action.
- Ensures originally/derivatively classified documents are properly marked.
- Conducts security assessments to ensure proper classification, handling, accountability, safeguarding, and destruction.
- Serves as point of contact for security equipment for protecting classified information
- Responds to classification management questions/inquiries.

i. Personnel Security Specialist

- Initiates requests for security clearances based on staff need for access to classified information and ensures such persons complete required background investigation forms.
- Maintains personnel security records on individuals authorized access to classified information.
- Properly uses standard security forms.
- Ensures proper packaging when forwarding personnel security files. Attends training and keeps basic knowledge of handling requirements for classified information.
- Verifies clearances of persons requesting access to classified information.
- Ensures classified information is not provided to unauthorized persons.
- Reports any apparent or suspected attempt to access classified information by unauthorized persons and assists in official inquiries.

j. Office Support Assistant/Secretary

- Schedules staff to attend training on safeguarding requirements for classified information.
- Maintains office file records containing classified information and retrieves files relating to classification activity within Treasury/bureaus.
- Maintains and properly uses stock of standard forms to protect classified information.

- Ensures proper packaging when forwarding classified information.
- Attends training and has knowledge of essential requirements for classified information.
- Ensures receipts for classified are promptly signed and original copy returned to sender.
- Verifies clearances of persons requesting access to classified information.
- Ensures classified information is not provided to unauthorized persons.
- Assists in compiling information on classified documents generated annually.

k. General Employee with Security Clearance

- Attends training on and maintains understanding of safeguarding requirements for classified information.
- Ensures classified documents are properly marked.
- Maintains Top Secret document inventories, as warranted.
- Ensures that official contacts have the need-to-know classified information and appropriate security clearance.
- Ensures classified documents identify source(s) and dates/events for declassification.
- Properly uses standard forms to protect classified information.
- Ensures records are maintained on all use of classification authority.
- Verifies clearances of persons requesting access to classified information.
- Ensures classified information is not provided to unauthorized persons.
- Reports any apparent or suspected attempt to access classified information by unauthorized persons and assists in official inquiries.

Chapter III
Section 23

Automatic Declassification

Updated
6/4/14

1. Introduction

Permanently historically valuable information classified under Executive Order (E.O.) 13526 or a prior E.O. is subject to automatic declassification upon reaching 25 years of age. Such classified records will automatically be declassified on December 31st of the year that is 25 years from its date of origin. This section establishes Department of the Treasury requirements for reviewing classified information as it approaches (and in advance) of its reaching 25 years of age.

The automatic declassification provision does not apply to records containing Restricted Data (RD) or Formerly Restricted Data (FRD) that are classified under the Atomic Energy Act of 1954. RD and FRD information shall be referred to the Department of Energy and Department of Defense, respectively, for declassification purposes.

2. Authorized Holders

Authorized holders of classified information include the Departmental Offices (DO) and bureaus with original classification authority (or which previously had original classification authority) or that otherwise maintain classified records either on-site or secured in one or more records storage facilities. DO/bureau records routinely include classified information originated by other U.S. Government agencies or departments and/or foreign government information. Such records may be the source material upon which DO/bureau officials derivatively classify particular information. The automatic declassification review process applies to DO/bureau originated classified information and also information derived from other agencies and departments that is classified.

3. Treasury and Bureau Record Locations

a. *Washington, DC Area Storage.* Classified records are either preserved with the National Archives and Records Administration (NARA) in College Park, Maryland, temporarily stored at the Washington National Records Center (WNRC) in Suitland, Maryland or in active (or inactive) secure file storage in DO/ bureau space and held by other Federal agencies/departments in the Washington, DC area. Despite retention by NARA or the WNRC, DO/bureau officials are responsible for declassification decisions up to 25 years from the date of original classification. Such records are still subject to mandatory and/or systematic declassification review.

b. *Presidential Library Storage.* DO/bureau classified records are also held at various Presidential Libraries and include information contained in donated historical material or under deed-of-gift restrictions between a particular Presidential Library and one or more

(now former) DO/bureau officials generally reflecting that official's service and/or including the official's deeded private papers.

3. Waived Treasury Classified Equities

a. *Automatic Declassification in Bulk.* Office of Security Programs (OSP) inquiries throughout the entire Department in 2005 resulted in original classification authorities' concurrence in the bulk declassification of 25-year old classified records. This determination only applies to DO/bureau classified equities of strictly DO/bureau origin. The decision does NOT equate to automatic release of declassified records at 25 years of age as there may be requirements in the Freedom of Information Act and Privacy Act to withhold release of specific information covered by Federal statute.

b. *Other Agency or Department Classified Equities.* Notwithstanding the above determination, DO/bureau subject-matter experts are required to examine classified records generated by them that are stored at NARA, the WNRC, the Main Treasury and Annex Buildings and within DO/bureau-occupied space. This is to identify classified equities belonging to non-Treasury agencies/departments. Such reviews may involve employing cleared contractors to conduct line-by-line document reviews with assistance of employee subject-matter experts and ensuring attendant quality control reviews. Additionally, foreign government information that appears subject to automatic declassification or mandatory review shall also be referred by holders to the Department of State to determine whether it is subject to a treaty or international agreement that would prevent its declassification at 25 years of age. Where records are identified containing classified information originated by other agencies or disclosure of which would affect the interests or activities of other agencies, those records that could reasonably fall under one or more of the exemptions in Section 3.3b of EO 13526 (see paragraph 8 below) shall be referred to the originating agencies. Referrals require reviewing DO/bureau to provide formal notification to the originator(s), making the records available for their review and recording final agency determinations.

c. *Exceptions to Bulk Declassification.* Formal requests to retain classification beyond 25 years were approved for a limited volume of United States Mint and U.S. Secret Service (USSS) records under the Interagency Security Classification Appeals Panel (ISCAP) review process and do not need to be revisited. Per paragraph 6 below, classified records created by former bureaus are now to be treated as other agencies or departments information. The ISCAP review process requires the Director, OSP to formally submit information to the Information Security Oversight Office (ISOO) for approval as identified in paragraph 9 below and reviewed and updated as circumstances required, but at least once every five years.

d. *Failure to Re-review.* Where an exception has been approved by the ISCAP and the declassification date or event is well into the future, a re-review time frame must be established to verify the continued validity of "today's" need to exempt specific documents from automatic declassification. Failure of DO/ bureaus to re-review

documents by the prescribed declassification date or event time frame will result in the automatic declassification of the previously exempted information.

e. *File Series Exemptions.* When a review or assessment results in a determination that information within a file series almost invariably falls within one or more of the exemption categories in Section 3.3(b) of EO 13526, and the DO/bureau proposes to exempt such information from automatic declassification at 25 years, the Director, OSP shall be so advised by reviewing/assessing officials and the Director, OSP shall notify the ISCAP. The notification shall include a description of the file series; explanation of why information within the file series should be exempt and remain classified for a longer (recommended) period of time.

4. Departmental Offices and Bureau Review Responsibilities

DO/ bureau officials are responsible for coordinating with their records management officials to establish individual office records retention schedules for information they collect, analyze, generate and retain. Records schedules are generally prepared at the level of Assistant Secretary in DO and at the corresponding bureau level for applicable official records. DO/bureau offices that have generated and/or are currently in possession of classified information with dates starting at January 1, 1990 are individually responsible for reviewing their classified records holdings prior to temporary storage to the WNRC or final transfer to NARA.

This is to identify and label DO and/or bureau classified records subject to automatic declassification at 25 years of age and other agencies and departments classified equities within DO/bureau records before such records are boxed or otherwise packaged for transport to the WNRC or NARA. This responsibility stems from the DO/bureau expertise and material support for establishing the need to collect, generate, analyze and otherwise document the nature of their work and related activities in the conduct of official business and for which the records are created. As the subject matter experts, the originating DO/ bureaus engagement in the automatic declassification review process is essential. Accordingly, DO/bureau offices are responsible for providing available resources, funding, and may hire cleared contractors to conduct such reviews to identify DO/bureau and other agency/department classified equities within their records.

The same review process applies to active and inactive records containing classified information (regardless of origin) with dates starting at January 1, 1990, that are retained in DO/bureau occupied office space. Affected DO/bureau officials are further responsible for identifying and ensuring sufficient resource support and funding to review classified records they maintain within active and inactive records. This may include employing cleared contractors to conduct such reviews on their behalf to identify and label other agency and department classified equities within active and inactive records.

5. Declassification Review Decision Labeling

Treasury-originated classified documents containing DO/bureau equities that are subject to

automatic declassification and that are determined to be declassified at 25 years of age shall be so labeled. This shall be accomplished by affixing a pre-manufactured label identifying the authority as "E.O. 13526, the date of such action, and the words "Treasury Department" or originating bureau name followed by the name of the office making such determination and/or conducting the review. An example appears below:

DECLASSIFIED
Authority: E.O. 13526
Date: 17 June 2011
Treasury Department, Office of Security Programs

Where DO/bureau classified records holdings subject to automatic declassification contain classified equities of other agencies or departments, and there is no objection to declassification at 25 years of age, the reviewed documents shall also be so labeled. This shall be accomplished by affixing a Standard Form 715, *Government Declassification Review Tab*, to identify other agencies or departments whose classified equities are contained therein. Reviewers shall use the ISOO standardized abbreviations to identify the name(s) of non-Treasury agencies/departments, for example: DOS for State, DOD for Defense, USTR for U.S. Trade Representative, etc., so that it is clearly discernable which agencies or departments classified equities are involved. An example appears as follows:

No Department of the Treasury objection to declassification subject to (fill in abbreviated name(s) of other agencies/departments) concurrence.

6. Classified Equities of Former Treasury Bureaus

When classified information is transferred in conjunction with a transfer of functions, and not merely for storage or archival purposes, the receiving agency is deemed to be the originator. Accordingly, responsibility for automatic declassification review of classified equities generated by former Treasury bureaus resides with the receiving agency. Despite such classified records appearing on DO or bureau letterhead, Treasury has waived the need for former Treasury bureau classified equities to be reviewed by current DO/bureau officials. Reviewers shall standardize the manner in which they identify the name(s) of affected former Treasury bureaus, for example: USSS for the U.S. Secret Service, USCS for the U.S. Customs Service, ATF for the Bureau of Alcohol, Tobacco and Firearms, FLETC for the Federal Law Enforcement Training Center, USCG for the U.S. Coast Guard, BNDD for Bureau of Narcotics and Dangerous Drugs and Interpol.

7. Newly Discovered Classified Records

Treasury's decision to subject DO/bureau classified records to automatic declassification in bulk does not apply to DO/bureaus which have requested and been given an exemption by the ISCAP for specific categories or volumes of information. In the event newly discovered classified records are located, the finding DO/bureau has up to three years from the date of discovery to make a final determination with respect to declassification, exemption or referral (to another

agency or department). The Secretary of the Treasury or Senior Agency Official must consult with the Director, ISOO on any decision to delay automatic declassification of newly discovered records no later than 90 days from the discovery of the records. Such consultation shall identify the records, the volume, anticipated date for declassification, and circumstances of the discovery.

8. Authorized Exemptions

The following categories of information may be used as the basis for requesting an exemption from automatic declassification at 25 years of age and include specific information, the release of which could be expected to:

a. Reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

b. Reveal information that would assist in the development or use of weapons of mass destruction;

c. Reveal information that would impair U.S. cryptologic systems or activities;

d. Reveal information that would impair the application of state of the art technology within a U.S. weapon system;

e. Reveal actual U.S. military war plans that remain in effect;

f. Reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

g. Reveal information that would clearly and demonstrably impair the current ability of the United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

h. Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

i. Violate a statute, treaty or international agreement.

9. Requirements for Future Exemption Requests

Exemptions are not automatic or final until formally approved by the ISCAP. OSP will work with the requesting DO/bureau to fine-tune the request as may be necessary, handle liaison with the ISOO, coordinate with Treasury's Senior Agency Official and engage with ISOO throughout the ISCAP review and decision-making process. Only upon specific approval by the ISCAP

may a particular exemption be formally invoked. However, pending such decision the specific information will continue to remain classified. DO/bureaus requesting exemption of particular information from automatic declassification at 25 years of age shall coordinate such requests with the Director, OSP who shall coordinate with the ISCAP. The requesting DO/bureau office is responsible for identifying the following information:

a. Text format(s);

b. Levels of classification;

c. Volume and storage location(s);

d. Time frame by span of years;

e. Reason(s) why the information should be exempt, (either by reference to information in specific records or in the form of a declassification guide); and

f. Except for the identity of a confidential human source or human intelligence source, a specific date or event for declassification.

Chapter III Section 24 **Sensitive But Unclassified Information** Updated 5/16/14

1. Term "Sensitive But Unclassified"

The term "Sensitive But Unclassified" originated with the Computer Security Act of 1987. It defined SBU as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (USC) (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy." More recently, the Electronic Government Act of 2002 recognized the importance of information security to the economic and national security interests of the United States.

2. Primary Term for SBU Information

SBU shall be the primary term used to mark sensitive information originating in the Departmental Offices (DO)/bureaus. The SBU marking shall identify information, the release of which may adversely impact economic, industrial, or international financial institutions; or compromise unclassified programs or DO/bureau essential operations or critical infrastructures. Previous designations to label sensitive information like Limited Official Use, For Official Use Only, Market Sensitive, Close Hold, Eyes Only, Privileged or Proprietary, et al., shall not be used to identify SBU information produced within DO/bureaus unless a particular term is authorized by law, statute, or agency regulation or as identified in paragraph 5 below. SBU information so marked is not meant for public release but controlled or restricted in conducting official DO/bureau business.

Access to SBU shall be based on a determination that an employee, contractor personnel or consultant requires access to specific SBU information in order to perform or assist in lawful, authorized DO/bureau governmental functions; a security clearance is not required to access SBU information.

3. Categorizing SBU and Restrictions

Criteria and terminology defining the types of information warranting designation as "sensitive" varies across the Federal Government and such designations and use are discretionary. Foreign governments also share restricted information or provide sensitive information in confidence based on treaty, bilateral exchange agreements or other obligations.

Designation of particular information as "sensitive" is not a license to; (1) conceal possible negligence, waste or illegal activity; (2) prevent embarrassment to a person,

organization, or agency; (3) to restrain competition; (4) to prevent or delay the release of information; or (5) to restrict access by executive, legislative, or judicial agencies, organizations or officials.

4. Relationship to the Freedom of Information Act and Privacy Act

SBU information is not automatically exempt from provisions of the Freedom of Information Act (FOIA) or the Privacy Act. DO/bureaus components receiving a FOIA request for SBU or other sensitive information must evaluate the information and determine in each instance whether one or more FOIA exemptions apply. Such evaluation pertains to both marked and unmarked records that are subject to the FOIA. However, information sensitivity is expected to decrease with passage of time or changes in circumstances and this must be a factor in determining whether SBU information shall be released. The Privacy Act also requires agencies to collect, maintain, disseminate and make available to a person his/her personal information as required by the Act and its implementing regulations. SBU may include, but is not necessarily limited to, information:

a. Within international/domestic banking and finance sectors or otherwise protected by statute, treaty, or other agreements, or requiring protection until officially released.

b. Identifying DO/bureau unclassified critical infrastructures/key resources, protective measures for safeguarding information, facility schematics, etc.

c. Unclassified systems data, e.g., routing, configuration, engineering, systems-architecture, security surveys, personnel security files, or investigative type reports.

5. Exception for Law Enforcement Sensitive, Bank Secrecy, Tax Return Information and Other Agency Markings

Except for the term "LAW ENFORCEMENT SENSITIVE" used by other agencies and DO/bureau law enforcement components, e.g., Office of Terrorism and Financial Intelligence (TFI); Internal Revenue Service (IRS) Criminal Investigations (CI) Division; Office of Inspector General (OIG); Treasury Inspector General for Tax Administration (TIGTA); Special Inspector General for the Troubled Asset Relief Program (SIGTARP) the Financial Crimes Enforcement Network (FinCEN); and the Office of Foreign Assets Control (OFAC), descriptions similar to "Improper use of the report is a violation of 18 United States Code (USC) 641" used by the Comptroller of the Currency and the Office of Thrift Supervision (OTS) for bank exam/secrecy reports and "tax return information" restricted under Section 6103 of the Internal Revenue Code, no other terms shall be applied to DO/bureau-originated sensitive information determined to be SBU unless authorized by law, statute, or regulation.

Other Federal, State and local government agencies, international organizations or foreign governments may use different terms to identify their sensitive information. In most instances the safeguards are equivalent to SBU information. Some agencies and international organizations have additional requirements for their sensitive information. For example:

> Warning: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that might be exempt from public release under the Freedom of Information Act (5 USC522). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

DO/bureau users shall follow protective requirements of the U.S. Government agency/organization providing sensitive information but are not expected to re-mark such information. However, in responding to FOIA/Privacy Act requests for information, updated decisions as to the continued value or need to protect such information shall be noted on documentation for future reference prior to being returned to files. Employees shall contact non-Treasury originators of specifically marked SBU information for guidance or instructions on proper handling. In the absence of such guidance the information shall be safeguarded in accordance with the requirements contained in this section.

6. Responsibilities

DO/bureau employees, contractor personnel and consultants must be aware and comply with safeguarding requirements for SBU information. Personnel should also be aware that divulging SBU information without proper authority could result in administrative or disciplinary action (including contract termination). The lack of a SBU marking does not necessarily mean the information is not sensitive nor does it relieve the creator or holder of such information from responsibility to appropriately safeguard the information from unauthorized use or inadvertent disclosure.

DO/bureau officials who create SBU information are responsible for determining how long the information must be protected, for example, either by date or lapse of a determinable event. Unless otherwise noted on a document, information marked as SBU shall generally no longer be treated as sensitive after 25 years except as provided by statute, law or agency regulation. Previously generated sensitive information of DO/bureau origin shall be subject to release determinations under the FOIA/Privacy Act. Information creators, not system-operators, shall determine what information requires protection depending on the nature of the information and the environment is which it is processed and stored. SBU information shall not remain designated as such when its disclosure would no longer reasonably be expected to adversely impact economic, industrial, or international financial institutions; or compromise unclassified programs or

essential operations or critical infrastructures.
DO/bureau security officials shall provide routine oversight of measures in place to protect SBU information through a program of routine administration and day-to-day management of their information security program.

Supervisors and program managers are responsible for employees being trained to recognize and safeguard SBU information supporting their mission, operations and assets. Supervisors and managers shall also ensure an adequate level of education and awareness is maintained by affected employees. Education and awareness shall begin upon initial employee assignment and annually reinforced through mandatory training, staff meetings or other methods/media contributing to an informed workforce. This includes requiring appropriate security contract clauses for personnel, facilities and information protection through the acquisition process when access to SBU information is necessary.

Employees are also responsible for protecting SBU information supporting their mission, operations and assets. Protection efforts shall focus on preventing unauthorized or inadvertent disclosure and especially when visitors enter areas where SBU information is handled, processed, discussed or stored. This includes being aware of surreptitious and accidental threats posed by high-end communications technologies carried/used by employees and visitors, such as cell phones (with or without photographic capability), personal data assistants, portable/pocket computers, cameras and other video imaging recorders, flash/thumb drives, multi-functional and two-way pagers, and wireless devices capable of storing, processing or transmitting information.

Contracting officials, program managers, and technical assistants are also responsible for requiring appropriate security contract clauses for personnel, facilities, and information protection through the acquisition process of contracts or grants that concern access to SBU information.

7. Marking Requirements

Information designated as SBU and requiring such marking as determined by DO/bureau components and especially those identified in paragraph 5 above shall be distinctly labeled so persons authorized access are readily aware of its sensitivity. The lack of SBU markings, however, does not relieve the holder from safeguarding responsibilities. Unmarked SBU information already in records storage does not need to be removed, marked, and restored. However, when individual items are temporarily removed from storage that have no markings (and are subsequently deemed to be SBU) they shall be appropriately marked to reflect the correct status as SBU before being re-filed. Items containing SBU information shall be:

a. Prominently marked at the top/bottom of the front/back cover and each individual page with the marking "SENSITIVE BUT UNCLASSIFIED" or "SBU." Information system prompts may be adjusted to incorporate SBU markings in headers and footers.

b. Portions, paragraphs and subject titles containing SBU information shall be marked with the abbreviation (SBU) to differentiate it from the remaining text. Only when the entire text contains SBU information are individual portion markings optional.

c. Controlling, decontrolling or originator information markings are not required.

d. When sent outside DO/bureaus, SBU information documents shall include a statement alerting the recipient in a transmittal letter or directly on the document containing SBU information, for example:

> This document belongs to the Department of the Treasury (or cite bureau name). It may not be released without the express permission of (cite creating office or bureau). Refer requests and inquiries for the document to: (insert name and address of originating office/bureau and contact number(s)).

8. General Handling Procedure

Protective measures start when markings are applied and end when such markings are cancelled or the records are destroyed. SBU information may be reproduced on regular office copiers to the extent needed to carry out official business. Flawed or otherwise unusable reproductions shall be destroyed via shredding or placement in burn-bags. Although SBU is Treasury's standard for identifying sensitive information, some types of SBU information might be more sensitive than others and warrant additional safeguarding measures beyond the minimum requirements established herein. Certain information might be extremely sensitive based on repercussions if the information is released or compromised – potential loss of life or compromise of a law enforcement informant or operation. DO/bureaus and employees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property/equipment as the basis for determining the need for safeguards in excess of the minimum requirements contained herein.

a. A green "SENSITIVE BUT UNCLASSIFIED" cover sheet shall be used to prevent unauthorized or inadvertent disclosure when SBU information is removed from an authorized storage location and persons without a need-to-know are present or casual observation would reveal SBU information

b. When forwarding SBU information, an SBU cover sheet shall be placed inside the envelope and on top of the transmittal letter, memorandum or document.

c. When receiving SBU or equivalent information from another U.S. Government agency, it shall be handled in accordance with the guidance provided by the other U.S. Government agency. Where no guidance is provided it shall be handled in accordance with Treasury policy as described herein.

9. Dissemination and Access

a. Information designated as SBU shall be orally, visually, or electronically disseminated in such manner to avoid access by unauthorized persons. Precautions might include preventing visual access and restricting oral disclosure to designated individuals. Websites, if available to the public, shall not contain or provide links to SBU information.

b. Access to SBU information shall be on a need-to-know basis as determined by the holder of the information. However, where there is uncertainty as to a person's need-to-know, the holder of the information shall request dissemination instructions from his or her next level supervisor or manager.

c. Holders of SBU information shall comply with any additional access and/or dissemination restrictions cited on the document.

d. Unless marked to the contrary, SBU information officially released to Treasury/bureaus may be provided to another U.S. Government agency without prior permission of the originator.

10. Storage

a. SBU information shall be stored, at a minimum, in a file cabinet, desk drawer, overhead storage bin, credenza, or similar locked compartment. SBU information may also be stored in a room or area with physical access control measures affording adequate protection and preventing unauthorized access by the public, visitors, or other persons without a need-to-know. Examples include, but are not limited to, a key-locked room, or restricted access work area controlled by a cipher lock or card reader.

To the extent possible, SBU information stored in the same container used for safeguarding classified information shall be filed separately from classified information. However, when SBU and classified information are co-mingled in a DO/bureau document or file, the required protection for the particular file will be governed by the highest level of classified information.

b. Processing SBU information shall comply with Treasury/bureau systems security requirements for use of DO/bureau-owned or -leased equipment. When laptop computers are not being used, the laptop shall be stored to protect it from loss, theft, and unauthorized access. Information contained therein or stored on removable disks shall also be labeled and protected from unauthorized disclosure.

11. Transmission

a. *Within the U.S. and Territories.* SBU information to be transmitted within the United States and its territories shall be in a single opaque envelope/container and sealed to prevent inadvertent opening and to reveal evidence of possible tampering. The envelope/container shall bear the complete name and address of the sender and intended recipient or program office. SBU information may be opened and examined by mail room personnel in the same manner in which other incoming mail is evaluated and determined to be safe for internal delivery. SBU information shall be mailed by U.S. Postal Service (USPS) First Class Mail. Use of express mail services or commercial overnight delivery service is authorized, as warranted.

b. *Overseas.* When sent to overseas offices, SBU information shall be transmitted electronically and may be encrypted for purposes of transmission. If serviced by a military postal facility, i.e., APO/FPO, SBU information may be mailed directly to the recipient. Where the overseas office is not serviced by a military postal facility, the information shall be sent through the Department of State's (DOS's) unclassified diplomatic pouch. Advanced coordination with State officials shall be made to ensure delivery at the final destination meets Treasury/bureau needs and State's schedule for such deliveries.

c. *Via FAX.* Secure fax is encouraged for transmitting SBU information. However, SBU information may be transmitted via unsecured fax unless verbal or written restrictions have been cited by the originator. Where an unsecured fax is used, the sender shall be reasonably assured by the intended recipient that the information will not be left unattended or subject to possible unauthorized disclosure on the receiving end. Such assurance might entail the recipient standing by to receive SBU information and immediately phoning the sender to verbally acknowledge receipt. The recipient of the information shall comply with any access, dissemination, and transmittal restrictions cited thereon or verbally communicated by the originator.

d. *Via Secure Communication.* The use of a Secure Telephone Equipment (STE) is encouraged though not required. When using regular office telephones, users shall confirm speaking to an authorized person before discussing the information, and inform the person that the forthcoming discussion will include SBU information and identify those part(s) of the discussion that are sensitive. Only under exigent circumstances should voice-mail messages containing SBU information be left for a recipient. Thereafter, DO/bureau IT personnel shall be engaged to effectively delete such messages except where the message itself is regarded as evidence by a competent investigative authority.

e. *Via E-Mail.* Treasury/bureau internal e-mail systems provide sufficient safeguards to allow for the transmission of SBU information. However, it is up to the holder to determine if the information should be sent via e-mail or other means. If the

holder determines the information is too sensitive to transmit via e-mail, then it should not be sent electronically. Alternate secure arrangements must then be made to disseminate the information. If the holder determines e-mail provides sufficient protection, the information may be sent. For added security, the information to be sent may be included as an attachment rather than in the text of the message. The holder may then password-protect the attached file by activating the password capability of the word-processing program using a previously established password or a password sent to the intended recipient under separate cover.

12. Disposition

Originators and their successors may decontrol a record's SBU information status when circumstances indicate the information no longer requires protection. Known holders of the information shall be notified to the extent possible, that the information is no longer SBU and be directed to mark their copies accordingly.

13. Destruction

SBU documents shall be destroyed by burning, mulching, pulping, or pulverizing beyond recognition and reconstruction depending on the local jurisdiction's requirements. SBU information may also be destroyed by shredding or disposed of in burn bags. When shredding, the same equipment approved for destroying Secret and/or Confidential classified information shall be procured and used. If using burn bags, the outside shall be distinctly labeled or marked SBU to distinguish the contents from burn bags containing classified information. When using office shredders, employees are encouraged to dispose of the residue with normal paper waste in more than one trash receptacle to disseminate the remains as widely as possible. Treasury Publication 85-01, Volumes 1 and 2 at http://thegreen.treas.gov/programs/cyber/Pages/csp.aspx provides guidance and suggested methods for clearing or sanitizing various sensitive media.

14. Incident Reporting

a. Employees or contractor personnel who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of SBU information shall report it immediately, but not later than the next business day, to their supervisor and to local DO/bureau security officials. Notification to appropriate DO/bureau officials shall be made without delay when the disclosure or compromise could result in physical harm to an individual or compromise an unclassified plan or on-going operation. The initial notification may be either verbal or in writing.

b. The DO/bureau security official or designee shall conduct an inquiry to determine the details and prepare a report, copy of which shall be provided to the Director, Office of Security Programs, including the following:

- Whether or not an incident actually occurred. If there was no loss, compromise, or unauthorized disclosure, the security official shall so state.
- The responsible person(s).
- The cause of the incident.
- Actions taken to minimize damage or neutralize the potential for further compromise.
- Recommendations that can be implemented to prevent recurrence of similar incidents.
- The estimated impact.
- Any disciplinary action taken or planned, including training, to prevent recurrence.

Chapter III Section 25 — **Determining Sensitivity of Treasury Sensitive But Unclassified Information** — Updated 6/17/11

1. Introduction

This section implements Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated December 2003. The standards apply to all U.S. Government information other than classified information governed by Executive Order (E.O.) 13526 or the Atomic Energy Act of 1954, as amended, and all information systems other than those designed as national security systems. Security categorization standards in FIPS PUB 199 are intended to provide a common framework and understanding for expressing security that promotes:

- Effective management/oversight of information security programs, including coordination of information security efforts throughout civilian, national security, emergency preparedness, homeland security, and law enforcement communities.
- Consistent reporting to the Office of Management and Budget (OMB) and the Congress on the adequacy and effectiveness of information security policies, procedures, and practices.
- Corresponding guidance for Departmental Offices (DO)/bureau supervisors and managers in determining the sensitivity of particular program-related information warranting identification as "sensitive but unclassified (SBU)" and corresponding protection of information so marked.

2. Background

The term SBU shall be used to mark sensitive information originating within DO/bureau offices. SBU shall identify information, the release of which could cause harm to a person's privacy or welfare; adversely impact economic, industrial, or international financial institutions; or compromise unclassified programs or essential operations or critical infrastructures. Other caveats may be used when covered by law, statute, or regulation as identified in Chapter III, Section 24.

3. Security Categories

The E-Government Act of 2002 recognized the importance of information security in safeguarding U.S. economic and national security interests. Security categories are based on the potential impact on DO/bureau components should certain events occur that might jeopardize information needed by DO/bureaus to accomplish assigned missions, protect department-wide assets, fulfill legal obligations, maintain day-to-day functionality and

safeguard individuals. Security categories shall be used in conjunction with vulnerability/threat information in assessing Treasury/bureau risks and information types, i.e., privacy, medical, proprietary, financial, law-enforcement/investigative, acquisition-sensitive, security, or other types of information.

4. Responsibilities

Not all sensitive information merits individual protective marking. The benefits of marking are diminished if information is routinely marked as requiring particular attention/handling differently than other program information. DO/bureau supervisors and managers are responsible for determining information sensitivity and deciding at what impact level information within their respective component warrants being designated (and marked) as SBU, or might require some other designation authorized by law, statute, or regulation, or does not deserve any marking to identify its significance (or lack thereof) using the table below.

Supervisors and managers are responsible for ensuring their employees are advised about what types and categories of information warrant protection, marking, safeguarding, as well as restrictions (if any) governing use, collection, retention, and release of the information. On-the-job and/or other supervisor/manager-prescribed training shall make individual employees aware of the organization's rules with respect to determining sensitivity of official information and their obligations to protect it.

Employees are responsible for following DO/bureau organizationally-prescribed processes, practices, and procedures that apply to information so identified and marked as well as ensuring its protection.

5. Security Objectives and Impact

There are three security objectives for information (and information systems) under FIPS PUB 199 confidentiality, integrity, and availability. Confidentiality concerns preservation of authorized restrictions on information access and disclosure. Integrity guards against information modification or destruction, reliability and authenticity. Availability relates to timely and reliable access to or use of information or information systems.

a. *Low Impact* applies when the loss of confidentiality, integrity, or availability could reasonably be expected to have a limited adverse effect on Treasury/bureau operations, assets, or individuals. Examples might result in:

- Degradation of mission capability to an extent and duration that DO or a bureau is able to perform primary functions, but the effectiveness of the functions is noticeably reduced.

- Minor damage to DO/bureau assets.

- Minor financial loss.
- Minor harm to individuals (including, but not limited to, the loss of privacy as entitled by law).

b. *Moderate Impact* applies when the loss of confidentiality, integrity, or availability could reasonably be expected to have serious adverse effect on DO/bureau operations, assets, or individuals. Examples might result in:

- Significant degradation in mission capability to an extent and duration that DO/bureau is able to perform primary functions, but the effectiveness of the functions is significantly reduced.
- Significant damage to Treasury/bureau assets.
- Significant financial loss.
- Significant harm to individuals (including, but not limited to, the loss of privacy as entitled by law) but does not involve loss of life or serious life-threatening injuries.

c. *High Impact* applies when the loss of confidentiality, integrity, or availability could reasonably be expected to have a severe or catastrophic adverse effect on DO/bureau operations, assets, or individuals. Examples might result in:

- Severe degradation in or loss of mission capability to an extent and duration that the DO/ bureau is not able to perform one or more primary functions.
- Major damage to Treasury/bureau assets.
- Major financial loss.
- Severe or catastrophic harm to individuals involving loss or life or serious life-threatening injuries.

The following table shows potential low, moderate, and high impact definitions for security objectives based on confidentiality, integrity, and availability. Supervisors and managers shall establish organizational thresholds to determine when conditions warrant assigning sensitivity designations to identify (and mark) particular program information.

Security Objective	Low Impact	Moderate Impact	High Impact
Confidentiality Preserving authority restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	Unauthorized disclosure of information could reasonably be expected to have a **limited adverse effect** on DO/bureau operations, assets, or individuals.	Unauthorized disclosure of information could reasonably be expected to have a **serious adverse effect** on DO/bureau operations, assets, or individuals.	Unauthorized disclosure of information could reasonably be expected to have a **severe or catastrophic adverse effect** on DO/bureau operations, assets, or individuals.
Integrity – Guarding against improper information modification or destruction, reliability and authenticity.	Unauthorized modification or destruction of information could reasonably be expected to have a **limited adverse effect** on DO/bureau operations, assets, or individuals	Unauthorized modification or destruction of information could reasonably be expected to have a **serious adverse effect** on DO/bureau operations, assets, or individuals	Unauthorized modification or destruction of information could reasonably be expected to have a **severe or catastrophic adverse effect** on DO/bureau operations, assets, or individuals
Availability – Ensuring timely and reliable access to and use of information.	Disruption of access to or use of information or an information system could reasonably be expected to have a **limited adverse effect** on DO/bureau operations, assets, or individuals.	Disruption of access to or use of information or an information system could reasonably be expected to have a **serious adverse effect** on DO/bureau operations, assets, or individuals.	Disruption of access to or use of information or an information system could reasonably be expected to have a **severe or catastrophic adverse effect** on DO/bureau operations, assets, or individuals.

Chapter IV
Section 1

Contract Security

Updated
6/17/11

1. Purpose

This section establishes the security requirements for all contracts involving access to DO/bureau information, information technology and systems, facilities, and/or assets by contractors, licensees, certificate holders, and grantees, and their respective personnel.

This section implements the requirements of the Federal Acquisition Regulation (FAR), Office of Management and Budget (OMB) guidance, National Institute for Standards and Technology (NIST) publications, and related national policies applicable to classified and sensitive information. It also implements the National Industrial Security Program (NISP) for classified contracts as required by Executive Order 12829 as amended and it's implementing directives.

2. Scope

This section is applicable to all DO/bureau classified and sensitive contracts for products and services. It applies to all contract types, from credit card purchases and simplified acquisitions to major systems acquisitions.

DO/bureaus, including those bureaus exempted in accordance with Treasury Directive 12-11, Procurement Authority, shall ensure the security requirements of this section are implemented in all aspects and throughout the entire life cycle of each contract for a product or service, from inception of the need for a product or service to its final disposition.

Contract security is comprised of the following elements.

- *Program Security.* Security measures applied within the procuring office to protect information and assets during the acquisition planning, solicitation, award, and contract administration processes.

- *Contract Security Administration.* Security considerations incorporated into the contracting and administrative processes, such as acquisition security planning, contract security clauses, and security guidance to contractors throughout contract performance.

- *Product Security.* Security features incorporated into the acquired product or service.

- *Industrial Security.* Security requirements implemented by contractors and

subcontractors to safeguard information and assets they access or generate in the performance of a contract.

a. *Contractor definition.* Contractor means any industrial, education, commercial, or other entity, to include licensees or grantees, engaged in a contract with DO/bureau to provide a product or service.

3. Roles and Responsibilities

a. *Assistant Secretary (Management), Bureau Heads, Inspector General, Inspector General for Tax Administration, Special Inspector General for the Troubled Asset Relief Program and Senior Procurement Executive.* As it relates to their respective DO/bureau organization, the above named entities shall:

- Incorporate the security requirements of this section into acquisition regulations and policies.
- Ensure compliance with these security requirements within respective contract administration programs established pursuant to Treasury Directive 12-11, Procurement Authority.
- Identify a Designated Security Official (DSO) in writing to the Director, Office of Security Programs (OSP). Multiple DSOs may be necessary to promote efficiency. Each DSO should be an employee of the security component within their employing DO/bureau organization.
- Ensure contracting officers (CO), contracting officer's technical representatives (COTR), and other personnel responsible for contracts receive appropriate education and training concerning the requirements of this section.
- Ensure records are maintained of DO/bureau contractor facility clearances and approvals and contractor personnel security clearances and background investigations.
- Coordinate solicitations and contracts requiring access to classified and sensitive information with the OSP.
- Ensure the proper safeguarding of DO/bureau information, information systems, assets and facilities accessed by contractors.

b. *Designated Security Officials.* DO/bureau DSOs are responsible for reviewing for compliance with the Treasury Security Manual, TD P 15-71, contract security planning, solicitation, security guidance, and security administration of contracts

requiring contractor access to information, information systems, facilities, or assets under their purview. For classified solicitations and contracts, the DSO shall:

- Oversee the review of contractor operations within DO/bureau facilities.
- Review and/or certify all DD Forms 254, (Contract Security Classification Specification) signifying that security and classification guidance is appropriate and adequate, and submit all DD Forms 254 to the OSP prior to issuance for a solicitation or contract.
- Verify eligibility of contractors for access to classified information, including the verification of contractor classified mailing address as needed, and initiating sponsorship of facility security clearances as necessary.
- Review contractor visit authorizations submitted for classified solicitations and contracts.

In addition to initial and ongoing reviews of each classified and sensitive contract by the DSO, DO/bureau organizations shall establish procedures whereby DSOs are notified of the following events.

- Changes to contract security requirements or contract performance that affect security of the contract.
- Prior to invoking stop work orders, terminations-for-cause or for the benefit of the government, or other unplanned delays in contract performance.
- Conducting inspections of contractor facilities at the end of contract performance whenever a contractor had received, stored, or processed classified or sensitive information within their facilities.

c. *Treasury's Office of Security Programs*. The role of the OSP for classified contracts is to: (1) review DD Forms 254 submitted by DO/bureaus; (2) liaison with DSS on behalf of DO/bureau organizations on all NISP issues; (3) assist with verification of contractor eligibility for access to classified information; (4) coordinate DO/bureau initiated facility security clearance requests with the Defense Security Service (DSS); and (5) oversee DO/bureau compliance with the NISP.

d. *Defense Security Service*. While DSS has no direct role in the administration of contracts, it is charged as the Executive Agent for the NISP. DSS administers contractor security programs under the NISP by performing the following functions.

- Grants and oversees contractor Facility Security Clearances (FCLs) and personnel security clearances (PCLs).
- Assists newly cleared contractors with establishing security programs and secure facilities.
- Provide copies of the National Industrial Security Program Operating Manual (NISPOM) and related security requirements and forms to contractors.
- Monitors effectiveness and compliance of contractor security programs by providing assistance, conduct reviews/investigations
- Performs periodic inspections of contractor facilities and security programs.

e. *Contracting Officers (CO)* are responsible for ensuring all security requirements of law, executive orders, regulations, and applicable policies are met, and that security requirements are properly communicated and implemented through each contract and procurement vehicle. This includes all contracts, subcontracts, and procurement actions involved in each acquisition. Representatives of the CO may also fulfill some of these roles.

f. *Contracting Officer's Technical Representatives (COTR's)*, as it relates to their respective contracts, are responsible for determining the sensitivity of the information or accesses involved in the acquisition; ensuring adequate budget for necessary product and industrial security needs; incorporating security requirements (via preparation of DD Form 254 in conjunction with the responsible Program Manager) into acquisition planning and schedules; and ensuring security is implemented throughout the acquisition lifecycle. COTRs are responsible for providing acquisition security, product security, and industrial security requirements to the CO and necessary liaison with DO/bureau security officials. In addition, COTRs are responsible for:

- Approving or disapproving access for contractor personnel based on adjudication decisions made by personnel security officials.
- Tracking contractor access requests, background investigations, access approvals and disapprovals,
- Ensuring contractor accesses are appropriately terminated and in a timely manner, including the prompt return of identification, access control media such as cards and keys, the changing of combinations, information system user accounts, etc.,

- Ensuring only authorized contractors access information, information systems, assets and facilities
- Approving and monitoring contractor security programs and operations, including security plans and facilities, in coordination with DO/bureau physical security officials or the DSO.
- Ensuring approval of contractor information systems by appropriate authority, prior to processing DO/bureau information, and the proper termination of information systems at completion of need to process DO/bureau information.
- Ensuring security review of contractor information systems by appropriate authority during contract performance and at contract termination, and of contractor facilities at contract close out.
- Ensuring contractor personnel security clearances that are required for visits to DO/bureau facilities and involve access to classified information are certified to the responsible personnel security office.
- Tracking contractor personnel security clearances for visiting contractors and contractors working on-site.

4. Contracting Officer and Contracting Officer's Technical Representative Security Training

32 CFR Section 2004.22, NISP Directive 1, requires the Treasury Department to "ensure applicable department and agency personnel having NISP implementation responsibilities are provided appropriate education and training." DO/bureau COs and COTRs shall receive contract security training that includes the requirements of this section and in particular the NISP and NISPOM as well as how to complete DD Form 254 (Contract Security Classification Specification) for all classified contracts.

This training shall provide: (a) an overview of the various security requirements of the FAR, OMB guidance, and the NISP/OM; (b) acquisition security planning identified in this section: and (c) industrial security requirements of Chapter IV, Section 2. Contract security training shall be provided consistent with the schedule for all other COTR training and retraining.

5. Personnel Security in Connection with a Contract

All personnel responsible for (a) providing guidance to or overseeing performance of, or compliance by, a contractor, or (b) receiving or evaluating contract deliverables, shall be subject to a background investigation and/or personnel security clearance. The scope/level of the background investigation and/or personnel security clearance shall be

equal to or greater than that required for any respective contractor personnel or contract deliverable. This requirement applies to all information or accesses for which the contractor is required to have a background investigation or personnel security clearance.

Government and contracted or outsourced acquisition administration positions that are subject to this requirement include, but are not limited to: COs, COTRs, DSOs, Program Officials/Managers, and all financial, management, technical, engineering, and administrative support staff who are subject to the information and accesses within the scope of their respective responsibilities.

Example: A major system acquisition requires the scope of investigation of a Background Investigation (BI) for all contractor personnel in order to access the related computer system (while not needing a security clearance) and also a Secret personnel security clearance for a small number of contractor personnel to access a limited amount of classified documents. The CO, COTR(s), and program officials involved in this acquisition would require both a Secret clearance and a scope of investigation of BI. In this example, the minimum investigation of National Agency Check with Law and Credit (NACLC) for the Secret clearance must be supplemented or increased to a BI, so that the acquisition administration personnel have both the requisite clearance and background investigation.

6. Department-wide, Government-wide and Multi-Agency Contracts

Each procuring activity issuing a task order or delivery order through a contract administered by another agency or DO/bureau must ensure their respective security guidance and requirements are included in the task/delivery order(s). These security requirements must also include any non-disclosure agreements unique to the procuring activity.

All DD Forms 254 required for a task order or delivery order through a contract administered by another agency or DO/bureau shall be signed by a representative of the authority having security cognizance over the information, information systems, assets, or facilities accessed in the performance of the respective task/delivery order.

7. Security Cognizance of Classified Contracts

In accordance with an agreement between the Secretary of the Treasury and the Secretary of Defense, the Defense Security Service (DSS) is the Cognizant Security Agency (CSA) for DO/bureau contractors cleared under the NISP. Under this Agreement, DSS has cognizance over contractor-owned information systems and facilities operated on behalf of DO/bureaus, including those used incidental to contracts, unless specifically carved out of DSS responsibility in accordance with this Section. DO/bureaus retain security cognizance over classified information under its jurisdiction and over contractor operations and contractor owned information systems used within DO/bureau facilities and on DO/bureau property.

8. Acquisition Security Planning

Acquisition security planning will be conducted for all contracts involving access to DO/bureau information, information technology and systems, facilities, and/or assets by contractors, licensees, certificate holders, and grantees, and their respective employees. Acquisition security planning will determine security levels, conditions of contractor access, schedule, and security budget by identifying the factors given in Exhibit 1.

Acquisition security planning required of the Department of Treasury Acquisition Regulation (DTAR) and Federal Acquisition Regulation (FAR) will include both product and industrial security as applicable to the procurement action.

Procurement officials are cautioned that unnecessary costs and schedule delays often result when product security and industrial security are not adequately planned and implemented in the very beginning and throughout the entire acquisition process.

a. *Simplified Acquisitions*. The FAR does not require formal acquisition plans to record the acquisition security planning conducted for acquisitions within the threshold of Simplified Acquisitions, as defined by the FAR. However, acquisition security planning must be conducted to determine the same factors given in Exhibit 1 below, if those procurement actions involve (1) the procurement of information systems or technology, or (2) contractor access to classified or sensitive information, information systems, or assets.

Exhibit 1

Determine	*By Identifying These Factors:*
Security Levels	• Sensitivity of information, information systems, or assets to be accessed by contractors. • For contracts in which not all contractors will have the same need to access the same information, PM/COTR staff are strongly encouraged to develop a matrix of accesses. See Chapter II Section 3 for a model.
Personnel Security	• Background Investigations and/or personnel security clearances.
Conditions of Contractor Access	• Whether the access will take place at Treasury/bureau facilities only, at other government or contractor facilities, or at the contractor's or subcontractor's facility (requiring the contractor to establish a security program). • The various contractors involved in the acquisition, including the prime contractor, subcontractors, and consultants.
Physical Security	• Facility physical security requirements, including establishing secure areas or storage within contractor facilities.
Security Deliverables	• Contractor Security Plans defining the contractor security program and implementation of contract security requirements.
Schedule	• Lead time for background investigations and access approvals, secure

	facility construction and approval, acquisition of safes/storage containers, security approvals for information systems incidental to the contract, development and implementation of security awareness program, etc.
Security Budget	• Funds for background investigations (including initial and re-investigations) for contractor secure facility and for contractor security program and security staff. • Contract deliverables, such as the contractor security plan.

9. Contract Security Guidance

All contracts and procurement actions requiring the contractor to receive, generate, or otherwise have access to classified and/or sensitive information, facilities, information systems, or assets, will include appropriate guidance concerning the industrial security requirements of Chapter IV, Section 2. Solicitations and requests for proposals/quotes shall also include security guidance concerning the industrial security requirements identified in Chapter IV, Section 2 to ensure the U.S. Government receives realistic proposals and quotations.

Procuring activities shall ensure contract security guidance is evaluated throughout the entire life of the contract and adjusted to accommodate changes in access needs or security requirements applicable in every stage of the program.

a. *Security Levels.* All solicitations and contracts will identify the levels of classified or sensitive information the contractor will be required to receive, generate, store, and/or process (access), in order to respond to the solicitation or perform on the contract. These levels will be in accordance with the Federal Information Security Management Act (FISMA) or NISP; for smaller acquisitions, this guidance might only include the highest level. However, for larger acquisitions, the procuring activity should establish a matrix of accesses similar to that of Chapter II Section 3.

b. *Contractor Personnel Security Requirements.* Each solicitation and contract will identify contractor personnel security requirements as determined through the acquisition security planning process by the responsible COTR. This personnel security guidance will include position/access risk designations and the associated background investigations necessary for the access. Personnel security clearances will also be identified. The use of a position/risk matrix is strongly recommended. The personnel security requirements will include a listing of security forms all contractor personnel must execute for access approval. This list of forms does not need to include those forms submitted to DSS for the personnel security clearance.

c. *Information Security.* Each solicitation and contract will identify the information that needs protection. This includes all classified or sensitive information (1) contained within the solicitation or contract documents, (2) accessed in responding to the solicitation or performing on the contract, and (3) received or

generated by the contractor in connection with the solicitation or contract. Information security guidance shall include all appropriate instruction on authorized and unauthorized access, safeguarding, electronic processing, transmittal, storage and disposition. Such requirements are to be identified on DD Form 254.

d. *Conditions of Access.* Each solicitation and contract will identify the conditions under which the contractor will have access to the classified or sensitive information, information systems, facilities, and/or assets. The conditions will include the following information.

- Whether the contractor will access, safeguard and/or process information at (1) the contractor's facility(s), (2) DO/bureau, other government, or other contractor facilities as well, or (3) if ONLY at DO/bureau, other government, or other contractor facilities.

- Whether the contractor will be permitted to process information on government-furnished or contractor-owned information systems.

e. *Contractor Key Security Personnel.* All contracts shall require the contractor to assign and identify to the CO a key person(s) responsible for ensuring the contractor's compliance with contract security requirements. This person will also: (1) serve as the point of contact for the contracting activity to provide day-to-day security guidance and oversight, (2) ensure only approved contractor personnel access classified and/or sensitive information, information systems, facilities and/or assets, (3) coordinate adverse contractor personnel actions, (4) take immediate, unplanned security actions associated with the contract, and (5) be responsible for ensuring appropriate and adequate response to security incidents and violations.

f. *Contract Closeout, Final Disposition, and Significant Contract Events.* Contract guidance must include instructions for actions required at the conclusion of contract performance. This guidance will include instructions for retention or disposition of all information, U.S. Government-furnished equipment or property, and contractor-owned information systems storage media used to process sensitive information.

In addition, certain precautions must be taken when contract conditions change unexpectedly and have a potential adverse effect on contractor personnel, such as stop-work orders, layoffs, and labor disputes. Contracting activities must ensure that appropriate security precautions are implemented when contractor personnel are removed from the work place for such reasons. These precautions would include having combinations or locks changed, temporarily disabling access media and/or information system accounts, engaging more stringent system auditing, etc.

10. Oversight

Oversight and U.S. Government Access to Contractor-owned Facilities and Assets. DO/bureau contracting activities must conduct oversight of contractor security programs and operations for sensitive information and information systems. Oversight activities will be relevant only to the contractor operations, facilities, storage containers, work spaces, and information systems connected with the contract. See Attachment 1, Visiting Contractor Security Plan for Classified Information and Attachment 2, Visiting Contractor Security Plan.

a. *Within DO/bureau Facilities.* Contracts for which the contractor will work within DO/bureau facilities shall state the name(s) of the official(s) responsible for reviewing and overseeing the contractor's activities within DO/bureau facilities. The contracts will include provisions of government access to all contractor assigned work stations and areas, including desks, furniture, and storage cabinets, information systems accessed by the contractor, and all contractor-owned information systems used within the facility.

b. *Contractor-Owned Assets and Facilities.* Contracts for which contractor personnel receive, generate, store, or process DO/bureau sensitive information within their facilities must include guidance concerning oversight and compliance reviews to be conducted by the contracting activity. Routine or recurring reviews and oversight activities will be conducted every 12 to 24 months of contract performance, commensurate with prudent risk management. Such reviews will be coordinated with other known U.S. Government activities conducting reviews in order to reduce burden and impact on the contractor. Contracting activities should consolidate reviews, such as those for FISMA compliance and in accordance with this Section.

c. *Oversight of Classified Programs.* Procuring activities are required to oversee and review all contractor operations within DO/bureau facilities, including all activities involving classified information and information systems.

The Defense Security Service (DSS) has responsibility for oversight of contractor security programs for classified information used within contractor facilities. DSS reviews include all information and physical security, information systems security of contractor owned information systems, security awareness training, personnel security clearances, and visit authorizations, etc.

DO/bureau contracting activities will not conduct oversight visits or reviews of contractor operations and security programs for classified information within contractor facilities. If there is an incident warranting additional DO/bureau review or the unique perspective of DO/bureau security officials, such reviews will first be coordinated through the OSP, which will then coordinate with the responsible DSS field office as appropriate.

Visiting Contractor Security Plan for Classified Information

Contract Number:

Contractor: *{Insert Prime Contractor Name}*

Date of Original:

Revision Number: **Revision Date:**

1. INTRODUCTION

This Visiting Contractor Security Plan for Classified Information (VCSP/C) establishes security responsibilities and procedures for employees of *{Prime Contractor name}* working within *{Departmental Offices (DO) or bureau}* facilities and accessing classified and/or sensitive information, information systems, assets and/or facilities. This VCSP/C implements security guidance contained in contract number *{ # }* (hereafter "Contract", *{DO or bureau}* policies, the associated Contract Security Classification Specification (DD Form 254), the National Industrial Security Program Operating Manual (NISPOM), and the Treasury Security Manual, TD P 15-71, for the protection of classified and sensitive information, information systems, assets and facilities.

This VCSP/C is applicable to all *{Prime Contractor name}* employees and all of its subcontractor, vendor, and consultant personnel under this contract, (hereafter "Contractor"). The contractor shall require compliance with this VCSP/C in all subcontracts, labor purchases, vendor agreements, consultant agreements, etc., issued under this contract for which subcontractor, vendor, or consultant personnel will work within *{DO/bureau}* facilities and access classified or sensitive information, information systems, assets and/or facilities.

Security Responsibilities versus Contract Performance - Security requirements to be incorporated into or applied to the product or service provided by the contractor are identified in the contract. This VCSP/C identifies the security responsibilities of the contractor for working within *{DO/bureau}* facilities and to protect information, information systems, assets and facilities while producing the product or providing the service.

Contractor Security Plan - Unless otherwise directed by the CO/COTR and except as required in this VCSP/C, this VCSP/C constitutes all security plans and procedures for the contractor to work within *{DO/bureau}* facilities and no additional written security plans or procedures are required.

Review of this Plan - This VCSP/C shall be reviewed by both parties (Contractor and Contracting Officer), with assistance of the respective security officials, at least annually

and when changed conditions, such as in the program, facility, or statement of work, affect the security requirements for the contractor activities within *{DO/bureau}* facilities. Required changes to this VCSP/C shall be implemented in a modification to the contract and contractor personnel briefed on the changes in accordance with Section 4 below.

2. NOTIFICATION OF RESPONSIBLE OFFICIALS

Contractor Security Representative - The contractor shall provide written notification to the Contracting Officer (CO) of its On-Site Contractor Security Representative (OCSR), including any changes or extended absence of the OCSR. This person should have a regular presence on-site and will be the liaison to the *{DO/bureau}* Program Management Office (PMO) for all on-site security matters, including but not limited to: access authorizations and terminations, identification and access media, security awareness training, information systems security, safeguarding information and materials, combination and key control, and security violations and incidents.

Government Security - The CO shall ensure the contractor is provided written notification of the Contracting Officer Technical Representative(s) (COTR), program official and/or security official(s) responsible as the Government Security Representative (GSR) for on-site contractor security matters. Notification shall include any additional security office or activity responsible for specific security functions for the facility, such as access identification, material control, secure communications equipment control, etc.

3. SECURITY COGNIZANCE

All information, information systems, and assets within DO/bureau facilities, and all contractor activities within DO/bureau facilities related to safeguarding information, information systems, assets and facilities, are under the security cognizance of the Department of the Treasury.

The Defense Security Service (DSS) retains cognizance over contractor facility security programs, including personnel security clearances, visit authorizations and visit authorization letters (VALs), security awareness training, Contractor security plans, and all other security issues relative to contractor access to classified information. However, DSS is relieved of cognizance and inspection responsibility of all contractor operations within DO/bureau facilities and property. The procuring activity shall assume security cognizance and responsibility for inspection of all contractor activities involving classified information, information systems, and assets, within DO/bureau facilities.

4. SECURITY AWARENESS TRAINING

All contractor personnel must receive security awareness training concerning their security responsibilities under this VCSP/C. This security awareness training shall be in addition to that for personnel security clearances and special accesses required of the

NISPOM. The Contractor is responsible to ensure all employees, subcontractors, vendors, and consultants, receive the training. Initial training is required prior to working within any *{DO/bureau}* facility. Additional security briefings, i.e. for access to information systems, may be required and will be identified separately.

Training content shall be in accordance with the Treasury Security Manual (TD P 15-71) or DO/bureau security policies. Security awareness training shall at a minimum consist of an initial security briefing, an annual refresher briefing, and retraining on changes to this VCSP/C as they occur. This training is mandatory for access. Contractor employees not receiving this training shall be denied further access. The contractor shall develop and conduct a training program, including associated records, unless otherwise provided by the PMO/COTR or local security authority.

Training required for an information system, such as User Security Training, shall be in accordance with the security requirements for the particular system.

5. ACCESS to *{DO or bureau}*

Contractor access to *{DO/bureau}* facilities/property is limited to those persons specifically approved by the COTR/PMO and security officials. The contractor shall ensure the COTR/PMO is provided the required security forms sufficiently in advance to permit access approval. The specific procedures and security forms required for access will be provided by the COTR/PMO separately.

Visit Authorization Letters - The contractor shall ensure visit authorization letters are submitted and terminated for all Contractor personnel, including subcontractors, vendors and consultants in accordance with the NISPOM.

Permitted Activities - The contractor is provided workspace within *{DO/bureau}* facilities for the purposes of performing tasks on this contract. The contractor is prohibited from conducting any activities within these workspaces, within *{DO/bureau}* facilities, or on *{DO/bureau}* property, not specifically related to this contract. The contractor shall not introduce any information or materials into such facilities or onto such property not directly related to this contract, without specific authorization of the CO/COTR/PMO and Treasury/bureau security officials.

Identification and Access Control Media - Identification and access control media will be issued to contractors having a need to access *{DO/bureau}* facilities on a frequent and recurring basis, as determined by the COTR/PMO. All identification and access control media are the property of the Department of the Treasury and are subject to termination or confiscation by the COTR, PMO, security activity, or other Treasury authority. Unauthorized use of U.S. Government identification is subject to 18 U.S.C. 499 and 701 and punishable in accordance with 18 U.S.C. 1028.

Identification shall be displayed above the waist and in plain view at all times within Treasury facilities and property. Loss of identification or access control media must be reported immediately to the CO/COTR/PMO or security authority.

The contractor shall ensure contractor personnel access only those areas, rooms, facilities, information systems, assets, and information, for which they are specifically approved. This includes ensuring access control media and system user account privileges do not exceed the authorized accesses.

Termination of Access - The contractor shall establish a process which ensures notification to officials identified by the CO, such as the COTR, PMO and/or security activity, and disabling of facility and information system accesses, immediately upon determination that a Contractor employee no longer requires access to *{DO/bureau}* information, information systems, assets and/or facilities. When it is determined a contractor employee will have temporary absence exceeding 30 days, all physical accesses and system user accounts shall be disabled during the period of absence. When it is determined a contractor employee no longer requires access, all identification and access media and all materials and equipment in possession of or charged to the employee shall be returned immediately upon termination of access.

Inspection on Entry/Exit and Prohibited Items - All persons and vehicles entering and exiting DO/bureau property are subject to search. Specific search criteria are established uniquely for each facility and will be identified to the contractor separately. Unless specifically required in the performance of this contract, permitted by the Director, Office of Security Programs or Bureau Security Officer, or otherwise permitted by law, the following items and materials are prohibited on or within facilities and property owned, controlled or operated on behalf of DO/bureaus:

a) Illegal drugs, paraphernalia, alcohol, and contraband
b) Firearms, ammunition and other weapons
c) Explosive materials and incendiary devices
d) Tear gas, chemical agents, hazardous substances (mace and other personal protection devices must be specifically approved by the local security authority)
e) Pornographic, offensive and other materials inappropriate for the workplace
f) Privately owned cameras and electronic equipment, including computers, radios, electronic recording and/or transmission devices.

Exceptions to the above will be specifically identified by the CO/COTR/PMO separately. See also Information Systems below.

6. INFORMATION SYSTEMS

Treasury policy prohibits the use of privately owned information technology to process Treasury classified or sensitive information.

Use of Government provided information systems - Contractors shall access only those information systems specifically identified by the CO/COTR/PMO. Those contractor employees authorized to use U.S. Government owned/controlled information systems shall, prior to first use and periodically thereafter, receive a security briefing on proper security procedures and permitted and prohibited uses (See paragraph 4). Security awareness training shall be in accordance with Treasury Information Technology Security Program (TD 85-01) or DO/bureau security policies, and will include: policies concerning personal and internet use; virus protection; user accounts; modification of software and hardware; and rules of behavior for the system.

Except as otherwise required by and in accordance with this contract, contractor personnel are prohibited from accessing, copying, manipulating, deleting, or otherwise affecting information or data processed or stored by *{DO/bureau}* information systems.

Contractor employees shall follow all security and local use procedures established for each information system. The contractor shall ensure no contractor personnel use an information system without first receiving authorization and obtaining the required user training.

Use of Contractor provided information systems - Contractor owned information systems used to process classified information shall be in accordance with the National Industrial Security Program Operating Manual (NISPOM). Contractor owned information systems must be approved by the PMO prior to introducing or otherwise processing DO/bureau information. The requirements for protecting sensitive information or information systems will be identified separately by the PMO.

Unless specifically authorized by the local responsible security office, contractor owned and privately owned electronic equipment are prohibited within Treasury facilities. This includes all computers, computer equipment and accessories, storage media, software, communications equipment (i.e. cell phones), and all devices with recording and/or transmission capability. Recording capability includes but is not limited to capturing any form of image, sound, or electronic signal.

Contractor and privately owned equipment, including computers, storage media, portable storage devices, and all electronic devices, shall not be connected in any manner to any DO/bureau owned or controlled information system, without specific approval of the CO/PMO. The contractor shall ensure no classified information is introduced to any contractor owned information technology without specific CO approval. Treasury policy

prohibits the introduction to or processing of classified information on privately owned information technology.

7. PHYSICAL SECURITY

The contractor shall ensure compliance with locally established physical security procedures. In addition to accomplishing all security audit records, such as recording opening and closing of areas and containers, the contractor shall ensure:

a) Doors to areas for which access controls are in place remain closed
b) Rooms and areas are secured when not occupied
c) Alarm systems are activated and deactivated properly
d) Storage cabinets, safes and containers are secured when not continuously monitored
e) Materials, equipment and assets, requiring additional storage are secured properly
f) End-of-day security checks are performed, as needed.

Access Control Systems - Contractor employees shall ensure access control devices are properly used by all personnel to record all entrances and exits of employees as required for the facility/areas accessed, to include ensuring all other personnel entering or exiting with the contractor employee register that action as required for the area/facility.

Escorting Visitors - Contractor personnel authorized to escort persons within a facility or area must maintain line-of-sight control over visitors and ensure their identification is displayed in plain view at all times within the facility. Contractors performing escort duties are responsible for ensuring escorted visitors do not access any area, information, information system, asset, or facility; they are not specifically authorized to access.

Before allowing visitors to enter, the escort must notify all personnel in the area to be visited, and once inside, ensure that classified and sensitive information cannot be accessed aurally, visually, or physically by the visitor. Line-of-sight control does not apply to restrooms; however, persons inside restrooms must be informed that a visitor is inside so that classified or sensitive information is not disclosed during a conversation.

No more than six escorted visitors may be assigned to an escort at one time. Visitors must be accompanied to the exit upon completion of the visit to sign out and return identification. Escorts found to be negligent in their responsibilities will be subject to a security violation.

8. INFORMATION SECURITY

The contractor shall ensure compliance with locally established information security procedures. The Contractor is prohibited from removing materials or transmitting

information from *{DO/bureau}* facilities without specific permission of the CO/COTR/PMO and shall do so only in accordance with local security procedures. The Contractor shall ensure:

a) Storage of sensitive and classified information in containers approved by the local security authority
b) Protecting information from disclosure during use and applying appropriate cover sheets to printed materials
c) Destruction and disposal of information in accordance with local procedures and not disposing of sensitive or classified information in the trash
d) Marking printed and electronic materials properly
e) Not removing materials from the facility unless specifically approved to do so.
f) Transporting materials in accordance with local procedures, in proper containers and only with specific approval to do so
g) When specifically approved by the PMO, contractors hand carrying classified materials from Treasury facilities shall do so in accordance with the NISPOM. The contractor shall administer courier authorizations and briefings, including identification.
h) Transmitting information electronically or by fax in accordance with local procedures, with proper receipts, and only with specific authorization to do so
i) Disclosing information only to those persons with a need-to-know, and security clearance or access authorization determined by the PMO

9. REPORTS

The contractor shall report to the CO/COTR/PMO:

a) Changed conditions affecting the company, to include: change of ownership, including stock transfers that affect control of the company; change in operating name or address; all actions to terminate business or operations for any reason; imminent adjudication or reorganization in bankruptcy; investigation or indictment for illegal or inappropriate business practice; any material change, discussion, consultation or agreement that may lead to effective ownership or control of the company by a foreign interest
b) Changes in contract related subcontracts or vendor or consultant agreements
c) Any vulnerabilities or malfunctions of information systems, intrusion detection or access control systems/devices, or communications security equipment
d) Security violations or incidents involving or affecting the confidentiality, integrity or availability of information or information systems
e) Suspicious and foreign contacts, in accordance with Treasury policy
f) Adverse information concerning employees

g) Changes in employee status including death, change in name or marital status, change in citizenship status or becoming a representative of a foreign interest
h) Changes in the Contractor, subcontractor and vendor facility clearances

The contractor shall also provide to the CO/COTR/PMO in a timely manner copies of reports required of the NISPOM, as they relate to the contractor, subcontractor or vendor facility clearance and/or employees working on DO/bureau contracts.

10. SECURITY REVIEWS

The CO/COTR/PMO shall ensure security reviews of contractor operations are conducted by local security authorities. Reviews will be conducted at least annually and in the case of security violation or incident or other non-compliance with security requirements. The contractor shall permit U.S. Government reviewing authorities' access to all workstations, work areas, storage containers, desks and office furniture, materials, and information systems. Results of security reviews will be provided to the CO/COTR.

The Contractor shall conduct periodic self assessments to ensure contractor personnel are complying with this VCSP/C and local security policies. Findings of non-compliance will be reported to the CO/COTR.

11. SECURITY VIOLATIONS AND INCIDENTS

The contractor shall report security violations and incidents immediately on discovery to the PMO and/or local security authority. Material, assets or information technology found exposed or improperly controlled shall be safeguarded until proper authority assumes control.

Unless otherwise directed by the COTR/PMO, security violations and incidents will be investigated by the local security authority. Culpable contractor personnel are subject to restriction or revocation of access, and civil or criminal punishment in accordance with applicable law.

Reports made to the DSS or FBI, as provided by the NISPOM, shall also be provided immediately to the CO/COTR/PMO or responsible security office.

12. EMERGENCIES

The preservation of life and prevention of injury, the protection of property, and the restoration of order are the primary goals, in that order, during an emergency. DO/bureau facilities are subject to various emergency conditions that may result in evacuation from the area or facility, sheltering in place within the facility, or permitting emergency personnel to enter the area.

Contractor personnel must acquaint themselves with the applicable Occupant Emergency Plan which will describe specific actions to take within their work area.

In all cases, time and conditions permitting, prior to evacuating or permitting entry of emergency personnel, all employees should secure or log-off their workstation and secure their sensitive and classified materials. In the case of evacuation, facility security should be established as practical.

At the end of an emergency, all personnel should inspect their respective workstations and storage containers for damage or compromise. As soon as possible after return to a facility, contractor personnel must advise the Program Office or local security authority of any changes in the security capabilities of their facility or storage containers, or if their information systems, information, assets, or workspaces appear to have been compromised.

Visiting Contractor Security Plan for Non-classified Information

Contract Number:

Contractor: *{Insert Prime Contractor Name}*

Date of Original:

Revision Number: **Revision Date:**

1. INTRODUCTION

This Visiting Contractor Security Plan (VCSP) establishes security responsibilities and procedures for employees of *{Prime Contractor name}* working within *{Departmental Offices (DO) or bureau}* facilities. This VCSP implements security guidance contained in contract number *{_#_}* (hereafter "Contract", *{DO/bureau}* policies, and the Treasury Security Manual, TD P 15-71, for the protection of information, information systems, assets and facilities.

This VCSP is applicable to all *{Prime Contractor name}* employees and all of its subcontractor, vendor, and consultant personnel under this contract, (hereafter "Contractor"). The contractor shall require compliance with this VCSP in all subcontracts, labor purchases, vendor agreements, consultant agreements, etc., issued under this contract for which subcontractor, vendor, or consultant personnel will work within *{DO/bureau}* facilities.

Security Responsibilities versus Contract Performance - Security requirements to be incorporated into or applied to the product or service provided by the Contractor are identified in the Contract. This VCSP identifies the security responsibilities of the Contractor for working within {Treasury Office or Bureau} facilities and to protect information, information systems, assets and facilities while producing the product or providing the service.

Contractor Security Plan - Unless otherwise directed by the CO/COTR and except as required in this VCSP, this VCSP constitutes all security plans and procedures for the contractor to work within {DO/bureau} facilities and no additional written security plans or procedures are required.

Review of this Plan - This VCSP shall be reviewed by both parties (Contractor and Contracting Officer), with assistance of the respective security officials, at least annually and when changed conditions, such as in the program, facility, or statement of work, affect the security requirements for the contractor activities within {DO/bureau} facilities. Required changes to this VCSP shall be implemented in a modification to the

contract and contractor employees briefed on the changes in accordance with Section 4 below.

2. NOTIFICATON OF RESPONSIBLE OFFICIALS

Contractor Security Representative - The Contractor shall provide written notification to the Contracting Officer (CO) of its On-Site Contractor Security Representative (OCSR), including any changes or extended absence of the OCSR. This person should have a regular presence on-site and will be the liaison to the {DO/bureau} Program Management Office (PMO) for all on-site security matters, including but not limited to: access authorizations and terminations, identification and access media, security awareness training, information systems security, safeguarding information and materials, combination and key control, and security violations and incidents.

Government Security - The CO shall ensure the contractor is provided written notification of the Contracting Officer Technical Representative(s) (COTR), program official and/or security official(s) responsible as the Government Security Representative (GSR) for on-site contractor security matters. Notification shall include any additional security office or activity responsible for specific security functions for the facility, such as access identification, material control, secure communications equipment control, etc.

3. SECURITY COGNIZANCE

All information, information systems, and assets, within DO/bureau, and all contractor activities within DO/bureau facilities related to safeguarding information, information systems, assets and facilities, are under the security cognizance of the Department of the Treasury.

4. SECURITY AWARENESS TRAINING

All contractor personnel must receive security awareness training concerning their security responsibilities under this VCSP. The contractor is responsible to ensure all employees, subcontractors, vendors, and consultants, receive the training. Initial training is required prior to working within any *{DO/bureau}* facility. Additional security briefings, i.e. for access to information systems, may be required and will be identified separately.

Training content shall be in accordance with the Treasury Security Manual (TD P 15-71) and DO/bureau security policies. Security awareness training shall at a minimum consist of an initial security briefing, an annual refresher briefing, and retraining on changes to this VCSP as they occur. This training is mandatory for access. Contractor employees not receiving this training shall be denied further access. The contractor shall develop and conduct a training program, including associated records, unless otherwise provided by the PMO/COTR or local security authority.

5. ACCESS to *{DO/bureau}*

Contractor access to *{DO/bureau}* facilities/property is limited to those persons specifically approved by the COTR/PMO and security officials. The contractor shall ensure the COTR/PMO is provided the required security forms sufficiently in advance to permit access approval. The specific procedures and security forms required for access will be provided by the COTR/PMO separately.

Permitted Activities - The contractor is provided workspace within {DO/bureau} facilities for the purposes of performing tasks on this contract. The contractor is prohibited from conducting any activities within these workspaces, within {DO/bureau} facilities, or property, not specifically related to this contract. The contractor shall not introduce any information or materials into such facilities or property not directly related to this contract, without specific authorization of the CO/COTR/PMO and Treasury/bureau security officials.

Identification and Access Control Media - Identification and access control media will be issued to Contractors having a need to access {DO/bureau} facilities on a frequent and recurring basis, as determined by the COTR/PMO. All identification and access control media are the property of the Department of the Treasury and are subject to termination or confiscation by the COTR, PMO, security activity, or other Treasury authority. Unauthorized use of U.S. Government identification is subject to 18 U.S.C. 499 and 701 and punishable in accordance with 18 U.S.C. 1028.

Identification shall be displayed above the waist and in plain view at all times within Treasury facilities and property. Loss of identification or access control media must be reported immediately to the CO/COTR/PMO or security authority.

The contractor shall ensure contractor personnel access only those areas, rooms, facilities, information systems, assets, and information, for which they are specifically approved. This includes ensuring access control media and system user account privileges do not exceed the authorized accesses.

Termination of Access - The contractor shall establish a process which ensures notification to officials identified by the CO, such as the COTR, PMO and/or security activity, and disabling of facility and information system accesses, immediately upon determination that a Contractor employee no longer requires access to {DO/bureau} information, information systems, assets and/or facilities. When it is determined contractor personnel will have temporary absence exceeding 30 days, all physical accesses and system user accounts shall be disabled during the period of absence. When it is determined contractor personnel no longer requires access, all identification and

access media and all materials and equipment in possession of or charged to the employee shall be returned immediately upon termination of access.

Inspection on Entry/Exit and Prohibited Items - All persons and vehicles entering and exiting DO/bureau property are subject to search. Specific search criteria are established uniquely for each facility and will be identified to the contractor separately.

Unless specifically required in the performance of this contract, permitted by the Director, Office of Security Programs or Bureau Security Officer, or otherwise permitted by law, the following items and materials are prohibited on or within facilities and property owned, controlled or operated on behalf of DO/bureaus:

a) Illegal drugs, paraphernalia, alcohol, and contraband
b) Firearms, ammunition and other weapons
c) Explosive materials and incendiary devices
d) Tear gas, chemical agents, hazardous substances (mace and other personal protection devices must be specifically approved by the local security authority)
e) Pornographic, offensive and other materials inappropriate for the workplace
f) Privately owned cameras and electronic equipment, including computers, radios, electronic recording and/or transmission devices.

Exceptions to the above will be specifically identified by the CO/COTR/PMO separately. See also Information Systems below.

6. INFORMATION SYSTEMS

Use of Government provided information systems - Contractors shall access only those information systems specifically identified by the CO/COTR/PMO. Those Contractor employees authorized to use U.S. Government owned/controlled information systems shall, prior to first use and periodically thereafter, receive a security briefing on proper security procedures and permitted and prohibited uses (See paragraph 4). Security awareness training shall be in accordance with Treasury Information Technology Security Program (TD 85-01) or DO/bureau security policies, and will include: policies concerning personal and internet use; virus protection; user accounts; modification of software and hardware; and rules of behavior for the system.

Except as otherwise required by and in accordance with this contract, contractor personnel are prohibited from accessing, copying, manipulating, deleting, or otherwise affecting information or data processed or stored by *{DO/bureau}* information systems.

Use of Contractor provided information systems - Unless specifically authorized by the local responsible security office, contractor owned and privately owned electronic equipment are prohibited within DO/bureau facilities. This includes all computers, computer equipment and accessories, storage media, software, communications equipment (i.e. cell phones), and all devices with recording and/or transmission

capability. Recording capability includes but is not limited to capturing any form of image, sound, or electronic signal.

Contractor and privately owned equipment, including computers, storage media, portable storage devices, and all electronic devices, shall not be connected in any manner to any Treasury owned or controlled information system, without specific approval of the CO/PMO.

Contractor owned information systems must be approved by the PMO prior to introducing or otherwise processing Treasury information. The requirements for protecting information or information systems will be identified separately by the PMO. Contractor owned information systems used to process classified information shall be in accordance with the National Industrial Security Program Operating Manual (NISPOM).

7. PHYSICAL SECURITY

The contractor shall ensure compliance with locally established physical security procedures. In addition to accomplishing all security audit records, such as recording opening and closing of areas and containers, the contractor shall ensure:

a) Doors to areas for which access controls are in place remain closed
b) Rooms and areas are secured when not occupied
c) Alarm systems are activated and deactivated properly
d) Storage cabinets, safes and containers are secured when not continuously monitored
e) Materials, equipment and assets, requiring additional storage are secured properly
f) End-of-day security checks are performed, as needed.

Access Control Systems - Contractor personnel shall ensure access control devices are properly used by all personnel to record all entrances and exits of employees as required for the facility/areas accessed, to include ensuring all other personnel entering or exiting with the contractor employee register the action as required for the area/facility

Escorting Visitors- Contractor personnel authorized to escort persons within a facility or area must maintain line-of-sight control over visitors and ensure their identification is displayed in plain view at all times within the facility. Contractors performing escort duties are responsible for ensuring escorted visitors do not access any area, information, information system, asset, or facility; they are not specifically authorized to access.

Before allowing visitors to enter, the escort must notify all personnel in the area to be visited, and once inside, ensure that sensitive information cannot be accessed aurally, visually, or physically by the visitor. Line-of-sight control does not apply to restrooms; however, persons inside restrooms must be informed that a visitor is inside so that sensitive information is not disclosed during a conversation.

No more than six escorted visitors may be assigned to an escort at one time. Visitors must be accompanied to the exit upon completion of the visit to sign out and return identification. Escorts found to be negligent in their responsibilities will be subject to a security violation.

8. INFORMATION SECURITY

The contractor shall ensure compliance with locally established information security procedures. The contractor is prohibited from removing materials or transmitting information from *{DO/bureau}* facilities without specific permission of the CO/COTR/PMO and shall do so only in accordance with local security procedures. The contractor shall ensure:

a) Storage of sensitive information in containers approved by the local security authority
b) Protecting information from disclosure during use and applying appropriate cover sheets to printed materials
c) Destruction and disposal of information in accordance with local procedures and not disposing of sensitive information in the trash
d) Marking printed and electronic materials properly
e) Not removing materials from the facility unless specifically approved to do so.
f) Transporting materials in accordance with local procedures, in proper containers and only with specific approval to do so
g) Transmitting information electronically or by fax in accordance with local procedures, with proper receipts, and only with specific authorization to do so
h) Disclosing information only to those persons with a need-to-know and access authorization determined by the PMO

9. REPORTS

The Contractor shall report to the CO/COTR/PMO:

a) Changed conditions affecting the company, to include: change of ownership, including stock transfers that affect control of the company; change in operating name or address; all actions to terminate business or operations for any reason; imminent adjudication or reorganization in bankruptcy; investigation or indictment for illegal or inappropriate business practice; any material change, discussion, consultation or agreement that may lead to effective ownership or control of the company by a foreign interest
b) Changes in contract related subcontracts or vendor or consultant agreements
c) Any vulnerabilities or malfunctions of information systems, intrusion detection or access control systems/devices, or communications security equipment

d) Security violations or incidents involving or affecting the confidentiality, integrity or availability of information or information systems
e) Suspicious and foreign contacts, in accordance with Treasury policy
f) Adverse information concerning employees
g) Changes in employee status including death, change in name or marital status, change in citizenship status or becoming a representative of a foreign interest

10. SECURITY REVIEWS

The CO/COTR/PMO shall ensure security reviews of contractor operations are conducted by local security authorities. Reviews will be conducted at least annually and in the case of security violation or incident or other non-compliance with security requirements. The Contractor shall permit Government reviewing authorities' access to all workstations, work areas, storage containers, desks and office furniture, materials, and information systems. Results of security reviews will be provided to the CO/COTR.

The Contractor shall conduct periodic self assessments to ensure contractor personnel are complying with this VCSP and local security policies. Findings of non-compliance will be reported to the CO/COTR.

11. SECURITY VIOLATIONS AND INCIDENTS

The contractor shall report security violations and incidents immediately on discovery to the PMO and/or local security authority. Material, assets or information technology found exposed or improperly controlled shall be safeguarded until proper authority assumes control.

Unless otherwise directed by the COTR/PMO, security violations and incidents will be investigated by the local security authority. Culpable contractor personnel are subject to restriction or revocation of access, and civil or criminal punishment in accordance with applicable law.

12. EMERGENCIES

The preservation of life and prevention of injury, the protection of property, and the restoration of order are the primary goals, in that order, during an emergency. DO/bureau facilities are subject to various emergency conditions that may result in evacuation from the area or facility, sheltering in place within the facility, or permitting emergency personnel to enter the area.

Contractor personnel must acquaint themselves with the applicable Occupant Emergency Plan which will describe specific actions to take within their work area.

In all cases, time and conditions permitting, prior to evacuating or permitting entry of emergency personnel, all employees should secure or log-off their workstation and secure their sensitive and classified materials. In the case of evacuation, facility security should be established as practical.

At the end of an emergency, all personnel should inspect their respective workstations and storage containers for damage or compromise. As soon as possible after return to a facility, contractor personnel must advise the Program Office or local security authority of any changes in the security capabilities of their facility or storage containers, or if their information systems, information, assets, or workspaces appear to have been compromised.

Chapter IV
Section 2

Industrial Security

Updated
6/17/11

1. Purpose

This section describes the industrial security and related requirements of Departmental Offices (DO) and bureau contractors to protect classified and sensitive information, information systems, assets, and/or facilities accessed or generated in the performance of work on contracts, programs, bids, or research and development efforts. As used in this section the term "Contracts" includes all forms of acquisitions, including licenses and grants. Industrial security requirements are imposed upon contractor personnel (and subcontractors) through security guidance included in solicitations, contracts and modifications or amendments thereto.

2. Scope

Industrial security is an element of contract security as identified in Chapter IV Section 1. Contract security applies to all classified (and sensitive) U.S. Government information, facilities, assets, and information systems subject to the National Industrial Security Program (NISP), for safeguarding classified information.

3. Contractor Security Operations

Contractors provide products and services in four types of operations, each having its own security requirements and guidance. Contractor operations may be one or a combination of any of the following operations.

a. *Visiting Contractors*. Visiting contractors are those contractor personnel having workspace and/or employed within a DO/bureau facility for an extended period of time. Contractors shall abide by security requirements established by the security and procuring activities. These security requirements, including security awareness training, shall be established in a Visiting Contractor Security Plan (VCSP) in accordance with paragraph 17. See Chapter IV, Section 1, Attachments 1 and 2.

b. *Approved Contractor Facilities and Security Programs*. Contractors receiving and/or generating DO/bureau information, information technology, and/or assets at their facilities require an approved facility physical security and security program. When this type of operation involves classified information or

materials, the contractor must have a facility security clearance through the Defense Security Service (DSS). When this type of operation involves sensitive information, information systems, or assets, the contractor security program and facility must be approved by the procuring activity. In this type of operation, the contractor may establish and manage its own security program, including security awareness training.

c. *Work at Other Government or Contractor Facilities*. Contractor personnel working at other U.S. Government agencies or at other contractor facilities must have their security clearance and/or access authorization certified to the activity being visited via established personnel security channels with notification to the DO/bureau procuring activity. Visiting contractor personnel must abide by the security program established by the DO/bureau or contractor being visited. Generally, new security awareness briefings are required when visits occur over an extended period, for example, beyond one (1) year and when new contractor personnel are assigned to the contract. The procuring activity shall incorporate all security requirements, including those for security awareness training, into the contract or a VCSP.

d. *Intermittent and Short-Term Visits*. Generally, contractor personnel visiting DO/bureau facilities, or other U.S. Government or contractor facilities, in support of a contract do so for meetings and contract-related activities of short duration. Security guidance will normally include specific instructions on how to gain access to the facility, use of any identification or access media, procedures for receipt, accountability and removing materials from the facility, and Homeland Security Presidential Directive-12 (HSPD-12) procedures specific to the area(s) to be visited.

4. Contractor Security Representative

Contractors shall identify a Contractor Security Representative (CSR) for all contracts requiring access to DO/bureau information, information technology and systems, facilities, and/or assets. The contractor shall provide written identification of its CSR and an alternate CSR (ACSR) to act in the absence of the CSR, to the Contracting Officer (CO) and DO/bureau security component within 30 days of contract award. The contractor shall immediately notify CO and DO/bureau security officials of any change in its CSR designations.

The CSR shall be responsible for all contract-related industrial security matters, including but not limited to the following tasks.

- Receiving and acting on access authorizations and terminations;
- Controlling access to identification media used within the Contractor facility;
- Developing and conducting and/or ensuring all contractor personnel receive security awareness training;
- Ensuring information systems security for contractor-owned information systems and as required by the CO;
- Safeguarding information and materials;
- Overseeing combination and key control;
- Overseeing visit certifications;
- Reporting security violations and incidents; and, as applicable;
- Having an effective contractor facility security program.

5. Contractor Security Plan

A contractor approved to perform contract operations at its facility requiring receipt, storage, generation, transmittal or destruction of classified and/or sensitive information shall develop a written security plan implementing all requirements of the Treasury Security Manual (TD P 15-71) applicable to its facility(s) and operations. The Contractor Security Plan (CSP) shall be a contract deliverable at the direction of the CO and shall be available for review by DO/bureau security officials. The CSP shall address, at a minimum, requirements and procedures for authorized access to information, facility access control procedures, facility open/closed procedures, security awareness training, visits and visitor control, information security, individual and corporate reporting requirements, security violations and incidents, and emergency procedures. The CSP shall include or reference contractor-owned information system security policies and procedures as required by the CO. The CSP shall include security policies and procedures applicable to classified information/materials and for sensitive information relative to the contract that implement requirements of the NISPOM and any unique requirements.

6. Contractor Security Awareness Training

In addition to the security education and training requirements of the NISPOM, the contractor shall ensure all contractor personnel receive security awareness training concerning their security

responsibilities commensurate with their involvement in the contract and their access to DO/bureau information, information systems, assets, and/or facilities. The contractor is responsible for ensuring all subcontractor, vendor, and consultant personnel also receive the training commensurate with their respective access(es). This training may be incorporated into the training given in accordance with the NISPOM.

Security awareness training shall be in accordance with the Treasury Security Manual and/or DO/bureau security policies. Information system user security briefings shall be in accordance with Part 12 of this Section.

a. *Initial Security Awareness Training.* Contractor personnel shall receive initial security awareness training prior to gaining access to DO/bureau information, assets, and/or facilities. Initial training shall include (1) an overview of the contract and the information, assets, or facilities needing protection; (2) personal-reporting obligations and requirements; (3) civil and criminal penalties for failing to properly safeguard information, assets, and/or facilities; and (4) security responsibilities and procedures applicable to the individual's job.

b. *Refresher Training and Periodic Updates.* The contractor shall ensure personnel accessing DO/bureau information, assets and/or facilities receive refresher training at least annually. The refresher training will reinforce the information covered in the initial training and provide updates on policies and procedures. Periodic updates shall also be provided that will support a continuing awareness program, update contractor personnel on security-related events, and provide notification of policy or procedure changes.

c. *Training Certifications and Records.* The contractor shall maintain a record of security awareness training they provide and retain copies of the training materials used and/or provided along with the original signature copy of acknowledgements by each individual. Electronic signature records of training may be used with specific approval of the DO/bureau contracting activity. Unless otherwise directed by the CO, records shall be kept for the duration of the contract, to include extensions, exercised options, and follow-on contracts and related delivery/task orders.

7. Contractor Personnel Security

a. *Requirements and Policies.* Contractor personnel security requirements for each contract are determined through the acquisition security planning process by the DO/bureau program officials responsible for an acquisition. Program officials must coordinate with DO/bureau security officials (including personnel security

officials) to determine appropriate position and access risk factors and to assign appropriate background investigations and mitigating personnel security policies. Personnel security policies concerning the scope of background investigations, reinvestigations, citizenship requirements, non-disclosure agreements, reciprocity of clearances and investigations between DO/bureaus and other agencies, adjudications, adverse information, access denial/revocation, and records for contractor personnel are identified in Chapters I and II.

b. *Access Approvals, Revocations, and Terminations.* Contractors shall limit requests for access to DO/bureau information, information systems, assets, and facilities to the minimum number of contractor employees necessary to fulfill contractual obligations.

(1) *Pre-Employment Requests.* Contractors shall not initiate pre-employment background investigation requests for prospective personnel without signed acceptance and commitment to work commencing within 180 days of the acceptance and in support of the DO/bureau contract, and with prior approval of the DO/bureau security component.

(2) *Access Records.* The contractor shall establish a record of access approvals, disapprovals, and revocations received for each individual on each DO/bureau contract or acquisition program. The records shall indicate the date of approval, applicable levels or types of access, effective date of termination of access(es), and denials and revocations of access. Records will also be kept of access approvals and termination of access for restricted access areas, assets, and information systems identified by DO/bureau contracting activities. Records of access approvals and terminations shall be retained and made available for inspection by DO/bureau officials for duration of the contract or longer as directed by the CO.

(3) *Access Termination.* The contractor shall terminate all physical and logical accesses by contractor personnel to DO/bureau information, facilities, assets, and information systems (1) immediately upon receipt of notice from the DO/bureau security component via the contracting activity that an individual's access has been revoked or suspended pending further action, and (2) upon determination that the individual no longer needs access to perform on the contract.

Termination of access includes disabling or otherwise preventing all physical and logical access to facilities, assets, and information systems operated on behalf of the DO/bureau, contractor-owned facilities in which DO/bureau information or assets are stored, and information systems processing or intended to process DO/bureau information. Access shall be terminated to the extent that contractor personnel no longer have unescorted physical or logical access or are otherwise unable to affect DO/bureau information processed or stored within the contractor-owned facility or information system. Termination of access includes the following actions.

- Disabling all information system user, group, and subsystem accounts used by contractor personnel, and changing individual and group passwords used by or known to the person.
- Disabling all physical access mechanisms, including access cards, changing combinations and codes, retrieving keys and other access devices, or changing the locks operated by those devices.
- Retrieving all identification and access media, such as access cards and keys.

(3) *Retrieval and Return of Identification and Access Media.* The contractor shall establish a process that ensures contractor personnel, upon termination of access, return all types of identification, cards, keys, or other devices used to gain physical or logical access to facilities or information system owned by or operated on behalf of DO/bureau, including all access media to other U.S. Government agency or contractor facilities and/or information systems, the contractor employee received in the performance of the contract.

c. *Disclosure of Treasury Information in Job Announcements, Resumes and Job Applications.* Contractors shall not disclose sensitive information in announcements for job vacancies supporting DO/bureau contracts. Personnel security requirements, such as the type of investigation, may be included to inform prospective applicants, using the following statement: "Applicants selected will be subject to a U.S. Government security investigation and must meet eligibility requirements for access to sensitive information." Contractor personnel may inform prospective employers about specific personal qualification

requirements by disclosing the type and date of any background investigations conducted by the DO/bureau. However, contractor employees must not disclose details of DO/bureau programs, including security requirements or status, locations, capabilities, or other sensitive data, in their resumes or employment applications.

d. *Contractor Personnel Security Clearances.* Except as provided for consultants and personal services contractors, contractor personnel security clearances shall be in accordance with the National Industrial Security Program Operating Manual (NISPOM).

8. Visits and Access Authorizations

Access authorizations for contractors visiting other DO/bureau contractors or U.S. Government agencies shall be certified through the DO/bureau security component. The CO may approve a contractor visit authorization process for visits between contractors with an existing contractual relationship or those involved in the same acquisition program.

a. *Visitor Access to DO/bureau Information, Systems, Assets, and Facilities.* Contractors shall permit access to DO/bureau information, information systems, assets, and facilities, including contractor-owned facilities operated on behalf of the DO/bureau, only to persons specifically authorized by the DO/bureau security component with notification to the procuring activity.

b. *Foreign Nationals.* The contractor shall report to the DO/bureau security component all visits by foreign nationals to contractor facilities in which DO/bureau information, information systems/technology, and/or assets are located. Contractors shall not permit access by foreign nationals to areas in which DO/bureau information technology or assets are located.

c. *Visit Records.* Contractors shall establish a record of visitors entering their facilities that includes the name and employer of the visitor, the date and times of the visit, and the purpose of the visit. Records of visits to contractor facilities involving access to DO/bureau information, information technology, and/or assets shall be retained and made available to DO/bureau security officials for two years or through contract closeout, whichever occurs first.

9. Physical Security of Unclassified Contractor Facilities

Contractors shall establish facilities constructed and secured in accordance with the Treasury Security Manual to protect all DO/bureau information, information technology or assets that are received, generated, or stored within contractor facilities.

a. *Contracted Security Services.* Contractors receiving contracted security services for their facilities, including but not limited to, alarm installation, maintenance and/or monitoring, guard forces, access control, lock and key services, or administrative security services shall have a legal contractual relationship with the provider of the security services. Providers of security services shall meet the citizenship requirements of the DO/bureau contract and have the requisite trustworthiness determinations and/or security clearances commensurate with their respective access.

b. *Co-Utilization of Contractor Facilities.* Contractors may co-locate DO/bureau information, information systems/technology, and assets with those of other U.S. Government agencies, provided security procedures are established and employees are aware of their responsibilities to separate DO/bureau information, information systems, and assets from those of the other U.S. agency(ies). The contractor shall receive CO approval prior to such co-utilization of contractor facilities. A Memorandum of Agreement shall be established between the DO/bureau procuring activity and the other U.S. agency that outlines security considerations for their respective information, information systems, and assets.

10. Facility Security Clearances

Except as provided in paragraph 14, a contractor must obtain a Facility Security Clearance (FSC) prior to gaining access to classified information. The FCL is an administrative determination that, from a security viewpoint, a contractor is a trustworthy business entity and is eligible to engage in contracts with the U.S. Government involving access to classified information. The FCL permits a contractor's personnel access to information classified at the level of FCL-granted and all lower levels.

A contractor engaging in contracts with the U.S. Government must first have a Company and Government Entity (CAGE) Code. The Defense Security Service (DSS), acting on behalf of DO/bureaus, will issue and track the FCL by the assigned CAGE Code. Detailed procedures on

the FCL process are provided on the DSS web site at www.dss.mil. However, Treasury's Office of Security Programs (OSP) should be contacted for assistance for procedures within DO/bureaus.

a. *Verifying Facility Clearances.* A contractor must have an FCL prior to any of its employees being granted access to classified information or material. Contractor FCLs are verified through the DSS' Defense Industrial Security Clearance Office (DISCO), Facility Clearances Division. The latest contact information for DISCO is available on the DSS website at www.dss.mil. However, Treasury's OSP should be contacted for assistance with verifying contractor facility clearances and current contact information for DISCO.

b. *Sponsoring Facility Clearances.* Upon determination that a contractor does not already have, and requires, an FCL to respond to a solicitation or perform on a contract, the procuring activity shall, through the Designated Security Officer (DSO) on the contract, inform the OSP for sponsorship of the contractor.

c. *Contractors with Foreign Ownership, Control, or Influence.* Facility security clearances for companies under Foreign Ownership, Control, or Influence (FOCI) shall be in accordance with the NISPOM, Chapter 2, Section 3. All national interest determinations (NID) required of NISPOM Section 2-309 shall be prepared by the procuring activity, approved by the responsible Treasury Assistant Secretary or Bureau Head, and submitted to the Director, OSP. The OSP shall coordinate all Special Security Agreements and Limited Facility Clearances with DSS, based on the submitted NID.

d. *Co-Utilization of Cleared Contractor Facilities.* Contractor facilities approved by the DSS or other Cognizant Security Authority (CSA) for safeguarding classified information shall be authorized to safeguard DO/bureau information and assets without further approval of the DO/bureau, upon review of the approving documentation by the OSP. To implement co-utilization, the contractor must provide a copy of the CSA written authorization for the facility to the CO and to the responsible DO/bureau security official.

When facilities that were approved by another agency are used, the contractor must immediately report to the CO and DO/bureau security component (1) any changes to the facility, including all changes affecting security status, changes in approval status, and temporary deficiencies or failures of security apparatus and (2) those mitigating measures in place. Contractors shall immediately notify the

CO and responsible security official, of the pending withdrawal of approval for contractor facilities that were approved by another agency authorized under this Section to secure DO/bureau information or assets.

11. Disclosure

Contractors shall safeguard DO/bureau information it receives or generates in accordance with the Treasury Security Manual, TD P 15-71.

a. *Disclosure.* Contractors shall not disclose the location nor permit access by persons unrelated to DO/bureau contracts or by foreign nationals to (1) contractor-owned facilities operated on behalf of the DO/bureau, (2) areas within contractor facilities housing contractor-owned information systems operated on behalf of DO/bureau, or (3) areas within contractor facilities housing DO/bureau information, information technology, or assets. Pre-contract meetings and negotiations with subcontractors, vendors, and consultants shall disclose only the minimum information and permit minimum access to assets or facilities necessary for proposals and pre-contract negotiations, in accordance with applicable security requirements.

b. *Public Release.* Public release of information concerning DO/bureau contracts or information is prohibited without prior approval of the procuring activity.

12. Information Systems (IT) Security

Contractors shall use contractor-owned information systems/technology to process DO/bureau information only with specific approval of the CO and in consultation with DO/bureau IT security officials. Contractor-owned systems shall be secured, receive certification and accreditation prior to processing, and be modified, maintained, and operated in accordance with the security requirements of Treasury Directive 85-01, Treasury Information Technology Security Program.

The CO may approve, with concurrence of the DO/bureau IT security officer, contractor-owned information systems secured and operated in accordance with other U.S. Government agency or non-U.S. Government national or international security standards. These non-DO/bureau standards must achieve the same protection required for confidentiality, integrity, and/or availability of DO/bureau information, as determined by the DO/bureau security and procuring activities. Such standards may be derived from American National Standards Institute (ANSI), International Organization for Standardization (ISO), or Institute of Electrical and Electronic Engineers (IEEE), or other recognized standards organizations.

The contractor shall not charge DO/bureau for the costs associated with information system security established by the contractor to implement non-Treasury security standards.

a. *Information Systems Security Reporting.* Contractors shall ensure possible or attempted penetrations of contractor-owned information systems used to process DO/bureau information are reported to the procuring activity and responsible DO/bureau security officials. When it is determined or suspected that the attempted or actual penetrations are directed at DO/bureau information, or resulted in loss of data confidentiality, integrity, or availability, the contractor shall also report to the responsible DO/bureau security office and the Director, OSP.

   Incidents of negligent, unintentional, and/or willful non-compliance with established security requirements by contractors, subcontractors, vendors, and/or consultant personnel shall be reported to the procuring activity responsible DO/bureau security office.

   All reports made to other federal, state, or local Government agencies concerning contractor-owned information systems used to process DO/bureau information shall also be reported to the DO/bureau procuring activity responsible DO/bureau security office.

b. *Classified Information Systems.* Contractor information systems used to process classified information shall be in accordance with the NISPOM or appropriate Director of National Intelligence Directive (DNID).

13. Reporting Requirements

a. *Contractor Reporting Responsibilities.* Contractors shall make the following reports through the CO to the responsible DO/bureau security office.

   - Changed conditions affecting the company, to include change of ownership, including stock transfers that affect control of the company; change in operating name or address; all actions to terminate business or operations for any reason; imminent adjudication or reorganization in bankruptcy; investigation or indictment for illegal or inappropriate business practice; any material change, discussion, consultation, or agreement that may lead to effective ownership or control of the company by a foreign interest.

- Changes in ability to safeguard DO/bureau information, information technology, assets, or facilities.
- Changes in contract-related subcontracts or vendor agreements.
- Any vulnerabilities or malfunctions of information systems (see paragraph 12 above), intrusion detection or access control systems/devices, or communications security equipment.
- Security violations or incidents involving or affecting the confidentiality, integrity or availability of information or information systems, or the unauthorized access to information, information systems, assets, or facilities.
- Suspicious and foreign contacts, in accordance with the Treasury Security Manual.
- Adverse information concerning contractor personnel, including information in cases of security violations or incidents.
- Changes in status of contractor personnel working on DO/bureau contracts, including death, change in name or marital status, change in citizenship status, or becoming a representative of a foreign interest.
- Any contractor personnel refusing to sign non-disclosure agreements required for access to DO/bureau information or who refuse to undergo required security awareness training.

b. *Contractor Personnel Reporting Responsibilities.* Contractor personnel approved for access to DO/bureau information, information systems, assets, and/or facilities, including those information systems and facilities operated on behalf of DO/bureau, shall make the following reports through the CO to the responsible DO/bureau security office.

- Name change.
- Psychiatric care.
- Arrests or convictions of any offense, including multiple minor traffic violations.

- Alcohol-related treatment or counseling.
- Serious financial problems.
- Drug abuse or use of illegal drugs, or related treatment or counseling.
- Contact with anyone exhibiting an unusual or inappropriate interest in their work for DO/bureau or in DO/bureau information, operations, assets, or facilities.
- Continuing contact with foreign nationals.
- Member of immediate family taking residence in a foreign country.
- Acquiring relatives through marriage who are citizens or residents of a foreign country.
- Changes in citizenship.
- Knowledge of security violations or incidents.

b. *Reports Required of the NISPOM.* All reports provided to the CSA concerning contractor personnel performing on DO/bureau contracts, information systems processing DO/bureau information, contractor security programs, and facilities also used for DO/bureau contracts, shall also be provided through the CO to the responsible DO/bureau security office.

14. Consultants and Personal Services Contractors

a. *Terminology.* A "consultant" is a person doing business in their own name or is a business entity owned by a consultant and/or a consultant and his/her immediate family with a single employee needing access. A " personal services contractor" is a person performing a personal services contract, including contracts for personal services provided by an expert or consultant, in accordance with Federal Acquisition Regulation Part 37.104, Personal Services Contracts.

b. *Status.* For security purposes, consultants contracting directly with DO/bureau and personal services contractors shall be treated as employees of the procuring activity. Consultants under contract to contractors shall be treated as an employee of the procuring company. The term "security purposes" includes personnel

security background investigations and adjudications; access authorizations, denials and revocations; non-disclosure agreements; and security awareness training. Consultants and personal services DO/bureau information at their residence or place of business, unless otherwise specifically provided by a facility security approval from the DO/bureau security and procuring activities.

c. *Personnel and Facility Security Clearances.* Consultants and personal services contractors shall not be authorized to receive, or store classified information at their residence or place of business, or to process classified information on their information systems, unless otherwise provided by a facility security clearance through DSS. Personnel security clearances will be administered in accordance with Chapters I and II of the Treasury Security Manual (TD P 15-71).

In very few contracts, only a single employee of a company not already cleared in the NISP might be required to have a personnel security clearance. A single employee of an un-cleared company may be cleared as a consultant with approval of the DSO and the OSP. Under this policy, the contract does not need to be a classified contract, therefore a DD Form 254 is not required and the company will not be sponsored for a facility security clearance (see paragraph 10). The procuring activity must ensure that only the single employee cleared by the DO/bureau is allowed access to classified information.

15. Subcontracting

Contractors shall ensure security requirements imposed by DO/bureau contracts are included in subcontract solicitations and contracts. The contractor shall receive approval from the procuring activity (in consultation with DO/bureau security officials) for all subcontracts requiring the subcontractor or vendor to receive, generate, or store DO/bureau information, information technology or assets prior to award of the subcontract. The contractor shall ensure subcontractor-owned information systems intended for processing of DO/bureau information are approved by the procuring and DO/bureau security activities prior to processing. Security standards for subcontractor-owned information systems that process DO/bureau information shall be in accordance with paragraph 12 of this Section, above. Prime contractors shall ensure all subcontractors DD Forms 254 are reviewed and approved by Treasury's OSP prior to issuance.

16. Oversight and Self-Assessment

Contractors shall cooperate with Federal agencies during official inspections, reviews, or investigations, and during the conduct of personnel security investigations of present and former

employees. Reviews will subject contractor personnel and all areas and storage containers under the control of the contractor to examination. The term "cooperation" includes providing suitable arrangements within the contractor facility for conducting private interviews of contractor personnel during normal business hours, providing relevant employment and security records for review, accompanying DO/bureau officials in the examination of the facility to include spaces and containers not authorized for storage of DO/bureau information or assets, and information systems not approved to process DO/bureau information.

The contractor shall conduct self-assessments of its security program periodically. The self-assessments will be commensurate with risk management principles and as directed by the CO. Self- assessments will include validating effectiveness of security equipment, facility and area construction, and compliance with security policies by contractor personnel.

17. Visiting Contractor Security Plans

A Visiting Contractor Security Plan (VCSP) or Visiting Contractor Security Plan for Classified Information (VCSP/C) may be used to identify all security policies and procedures applicable to contractor personnel working on-site within DO/bureau facilities for extended periods. The VCSP or VCSP/C should state all security procedures applicable to contractor personnel working on-site.

Solicitations should include the VCSP or VCSP/C to ensure that the bidding contractors include plans and costs for complying with security requirements. The VCSP or VCSP/C should be part of the contract and all changes and updates to the VCSP or VCSP/C after contract award made part of the contract via contract modification.

a. *VCSP and VCSP/C Templates.* The VCSP and VCSP/C templates are shown as Attachments 1 and 2 and shall be used by DO/bureaus. These templates must be modified by inserting the appropriate information, such as the contract number, contractor, procuring activity, and any specific security requirements applicable to the facility involved that are not already covered in the templates.

b. *Visiting Contractor Security Plans for Classified Information.* If the VCSP/C is used for classified contracts for which the contractor works on-site within DO/bureau facilities, it must be referenced in the DD Form 254.

Chapter V
Section 1

Security of Departmental Offices and Bureau Facilities

Updated
1/10/13

1. Introduction

This section establishes minimum standards of protection for Departmental Offices (DO)/bureau-owned and -leased buildings, compounds and facilities, including facilities operated by contractors on behalf of DO/bureaus. For this section, facilities include those for which DO/bureaus are responsible and that house Department of the Treasury personnel, assets and information.

2. Policy

Minimum protection for DO/bureau facilities shall be in accordance with Interagency Security Committee (ISC) security standards criteria. Security for DO/bureau facilities within the National Capital Region shall accommodate the design criteria of the National Capital Planning Commission (NCPC) report, *Designing for Security in the Nation's Capital*; dated October 2001, to the extent the incorporated designs achieve the protection objectives for the specific facility. The NCPC design specifications and recommend-dations shall be similarly considered for all facilities outside of the National Capital Region.

3. Facility Security Levels

Each facility will be designated Level I, II, III, or IV, in accordance with the ISC Standard, Facility Security Level Determinations for Federal Facilities, dated February 21, 2008, and appropriate security measures shall be implemented. A designation of Level V is reserved for and assigned only to those facilities identified and prioritized as national security critical infrastructure assets in accordance with the Treasury Critical Infrastructure Protection Program. A Level V designation necessitates implementation of extensive security measures and such designation requires coordination and concurrence of the Director, Office of Security Programs (OSP).

4. Leased Facilities

For GSA leased facilities, the GSA coordinates security assessments of proposed leased space for the appropriate security level and implements those security measures required by the GSA Standards for the Public Buildings Service. DO/bureau security officials

shall coordinate with the GSA and Federal Protective Service (FPS) and provide guidance through the facility security level (FSL) designation process when a lower or higher security level or additional security measures are determined to be necessary. Lease agreements for all GSA and non-GSA leased facilities must include provisions that ensure the DO/bureau occupant(s) have the flexibility and permission to modify the facility for security changes or enhancements throughout the period of the lease.

Security of leased facilities shall be consistent with ISC security standards. Personnel security requirements concerning access to facilities, information, information systems, assets, etc., apply equally to all persons regardless of employer. For example, if a DO/bureau leases a facility directly (non-GSA lease) they must require in the lease that all persons having the ability to access the leased space, including key utility areas, shall be subject to the appropriate personnel security eligibility standards consistent with the risk of their respective access.

5. Multi-Tenant Leased Buildings

Lease agreements for spaces in which DO/bureaus is not the primary U.S. Government tenant shall ensure that required security measures remain in place if the primary U.S. Government tenant vacates the facility or changes their security measures. Lease agreements shall ensure that security services established at a facility, shared by the DO/bureau tenant, are also available to that tenant. For example, when a DO/bureau lease agreement is established for space in a building already occupied by another agency which established on-site guard forces or alarm monitoring, the lease agreement shall ensure, if required by the DO/bureau tenant, that those on-site guard and alarm monitoring services are also available to and support the DO/bureau offices.

6. Security-In-Depth

Security-in-depth is defined as layered and complementary security controls sufficient to deter and detect unauthorized entry, movement, and activity within a facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), 24-hour operations, random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring, or other safeguards that mitigate the vulnerability of open storage areas without alarms and security containers during nonworking hours.

Security-in-depth shall be implemented for all facilities designated as Levels IV and V, and for those facilities housing information or information systems designated as High

Impact, in accordance with FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, and/or high-value assets identified in paragraph 16, below.

Comparable Security Measures. A comparable security measure is one that achieves a protection objective in lieu of a required measure stated in the Treasury Security Manual, TD P 15-71. For example, when security requirements include slab-to-slab wall construction for the purposes of controlling physical access to an area, a motion detector above the false ceiling could be used in lieu of wall construction when construction of the physical barrier is impractical. Comparable security measures are permitted when necessary and may be implemented only by senior DO or bureau security officials.

7. Assessments and Certifications

A security assessment process shall be established and maintained for all facilities to ensure implementation of the minimum safeguards of ISC Security Standards. Security assessments shall be conducted prior to occupancy and at intervals identified below. Vulnerabilities that cannot be corrected or mitigated through other measures, shall be reviewed by bureau security officers and the associated risk(s) accepted by the appropriate senior DO or bureau official. Security vulnerabilities not corrected prior to facility certification, as defined below, shall be documented. Plans of actions and milestones shall be established to correct the vulnerabilities as soon as possible. Additional security-in-depth or comparable measures shall be implemented to offset vulnerabilities until the conditions are corrected.

a. *Assessment.* Treasury facility security assessment programs shall include assessments conducted at intervals in accordance with ISC standards and any time there are significant changes made to the facility. At a minimum, assessments will be reviewed and updated as needed to accommodate minor changes at the following intervals:

- Level I and II, every five (5) years; and
- Level III, IV, and V, every three (3) years.

b. *Certifications.* A baseline of all security measures established for a facility shall be documented and certified by the senior DO or bureau official for the facility. Facility Security Certifications shall include a complete description of the facility, construction, and security measures, and include floor plans, site plans, and diagrams as necessary to support the facility and security description. Facility

Security Certifications will be used by the senior official to acknowledge the current documented facility security profile, the residual risks, and any recommended remediation. DO/bureaus shall implement a management process that ensures subsequent changes to a facility affecting the security certification have prior coordination and approval by the responsible security office.

Documented mitigation plans shall be used to support Facility Security Certification when the facility must be occupied and certain vulnerabilities require correction, as provided above.

8. Building Security Committees

A Treasury or bureau security representative and alternate (if available) shall be appointed to and participate in the building security committee (BSC) established for each building by the FPS in accordance with FPS Policy Directive FPS-05-002, Building Security Committees, dated February 16, 2005.

DO/bureaus shall ensure a BSC is established and maintained for their leased buildings and facilities not already having a BSC established by GSA or FPS. Ideal representation on the BSC will include expertise in security, facility management, architecture, engineering, and financial management. Membership of the BSC shall include, at a minimum, representatives of the building owner or management, a senior official of the tenant, and the locally responsible security authority.

In addition to those functions identified in the ISC Security Standards and FPS-05-002, BSC procedures shall provide the following functions:

- A means of communicating threat- or security-related notices to the facility population;
- Liaison to local law enforcement, fire, and other emergency response authorities, and established roles and responsibilities in responding to incidents and emergencies at each facility;
- Determination of appropriate security measures to be implemented during increased threat conditions; and,
- Review and adjustment of security measures as needed.

9. Security Plans and Operating Procedures

Security plans that document security operations and procedures for the facility shall be developed for each facility. These plans shall identify, at a minimum, the procedures for the following:

- Roles and responsibilities for the building security;
- Gaining access to, and opening and closing the facility;
- Visitor access to the facility;
- Alarm system operations and alarm response;
- Reporting security vulnerabilities and incidents;
- Increased threat conditions;
- Code Adam alerts;
- Function of facility-specific building security committees; and,
- Emergencies relative to physical security.

These procedures shall be coordinated with occupant emergency plans, security procedures applicable to information or assets stored within the facility, and other plans and procedures applicable to the facility. Security plans will be reviewed annually and updated as needed to accommodate changes in roles and responsibilities, changes in building security, or the change in building tenants which affect security plans.

10. Intrusion Detection Equipment and Systems

Installation, maintenance and operation of intrusion detection equipment (IDE) and systems (IDS) used to protect level III, IV, and V facilities shall be in accordance with, the requirements of Underwriters Laboratory (UL) Standard 1076 or UL Standard 2050. The FPS will provide assurances for alarm systems and monitoring for GSA-leased space. This requirement applies to all new installations. Existing systems, and those systems for which budgets were determined prior to October 2006, shall be made

compliant with this requirement as they are upgraded or replaced, but not later than October 2010.

Supplemental measures, such as additional detectors, closed circuit television (CCTV), or regular guard checks, shall be implemented for those systems not meeting the minimum requirements of UL 1076 or 2050.

Certificates and Inspections by UL. Both Standard 1076 and 2050 require UL inspectors to review, test, and certify alarm system installation, operations, and maintenance, and the alarm monitoring stations. The UL Standards also require installers to provide written certification of compliance with the Standard. Implementation of UL 1076 or 2050, in which the DO/bureau occupant provides its own monitoring station, or in areas in which UL inspectors will not be allowed as determined by the senior DO or bureau security official, will not require UL inspection. DO or bureau security officials shall notify the installation contractor upon contract award and coordinate the inspection limitations with the responsible UL representative (through the installation contractor) and the Director, OSP. DO/bureaus not permitting UL to inspect and approve installations and operations, must establish and maintain a self inspection, test, and certification process equivalent to the UL process for the standard used.

11. Identification and Access Media

All identification and access media, including the process of control, accountability, storage, issuance, revocation, and disposition, shall be in accordance with bureau implementation of Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 2004.

Access to all unused or blank stock of identification and access media, including ID cards, access cards, key fobs, etc., shall be permitted only by those persons with the requisite trustworthiness determination, need-to-know, and authorization to finish and program the identification/access media. All equipment used to finish and program identification and access media shall be secured and controlled commensurate with the access to be gained with the media. When identification or access media must be transmitted via U.S. Mail or other delivery service, sufficient controls shall be implemented to ensure only the authorized intended recipient assumes control of the media from the carrier. This includes restricted delivery and signature, similar to that required for national security classified material.

a. *Facial Images.* All pictures on DO/bureau identification media shall display the entire facial features of the subject. Persons with, temporary and medically required coverings, such as bandages, shall have their photographs taken once the coverings can be removed. Glasses worn by the subject when the picture is taken shall be prescription glasses required to be worn by the subject when entering, while inside and upon leaving facilities. Shaded or darkened glasses shall not be worn when the picture is taken.

b. *Covering the Face.* While entering and within facilities for security purposes, all persons shall ensure their face is uncovered at all times. Persons having temporary, medically required coverings of facial features, such as bandages, shall be required to identify themselves through other methods, as determined by the DO/bureau security official responsible for the facility.

c. *Display of Identification.* All persons entering DO/bureau facilities, and unless otherwise allowed by bureau security policy, shall display identification at or above the waist, in plain view at all times. Identification shall be removed from view upon exiting a facility. All persons shall surrender identification for verification of identity upon request at each facility entrance and any time within facilities.

12. Access after Regular Business Hours

After regular business hours and on weekends/holidays, employee badge-holders must sign in (and out) on the GSA or other Employee After-Hours Log-in Book upon entering and exiting the DO/bureau facilities. The badge-holder must identify their room and telephone number so that duty, uniformed, guard force personnel or emergency responders will be able to locate them in the event of an emergency. Weekend/holiday and after-hours contractor access must be submitted to appropriate security and/or administrative officials in advance of any work, e.g., repairs, installation, delivery or removal of furniture/equipment, etc., and include each person's name, date of birth, social security number, vehicle description along with the name(s) of the DO/bureau badge-holder providing escort.

13. Implementation of the Protect Act: Code Adam and Amber Alert Procedures

Treasury/bureaus shall develop and implement procedures for a child missing within their facility, in accordance with Title III, Subtitle D, of the *Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today* (PROTECT) Act of 2003, also known as the "Code Adam Act of 2003,". The Act, signed into law April 2003, requires "the

designated authority for a public building" to "establish procedures for locating a child that is missing in" a federal building. Once a child is determined missing "from" a federal building, an Amber Alert must be initiated in accordance with local procedures.

The GSA Public Building Service (PBS) administers and has the nation-wide lead in the Code Adam program for all GSA-leased facilities. DO/bureaus shall ensure Code Adam and AMBER Alert policies and procedures are established for facilities not under the control of GSA.

Implementation. The program and procedures established for Code Adam alerts shall provide, at a minimum, the following functions:

- Awareness training and instructions for employees on Code Adam alerts;
- A central point of contact for program administration in those facilities not under control of GSA;
- Points-of-contact to notify when a child is missing. For facilities without security forces, the points-of-contact should be the federal or contract guard forces, or designated officials, including alternates;
- Guidance for providing a detailed description of the child, including name, age, eye and hair color, height, weight, clothing, and shoes;
- Procedures for issuing a Code Adam alert and providing a description of the child using a fast and effective means of communication. Notification shall include the building management in leased facilities;
- Monitoring of all points of egress from the facility and building while a Code Adam alert is in effect;
- Conducting a thorough search of the building;
- Contacting of local law enforcement. Procedures shall include an immediate courtesy notification to local law enforcement;
- Actions that people should take once the child is located, including instructions if the child is found with someone other than his or her parent or guardian;
- Documenting the incident;
- Reporting the incident to local law enforcement if the search of the facility or building does not find the child in a reasonable time, for a determination to escalate to an AMBER Alert; and,
- Reporting the incident to the Director, OSP.

14. Prohibited Items

Unless specifically permitted by the senior DO/bureau security official, or Bureau Head, or as otherwise permitted or required by law, and as restricted by Department ethics and standards of conduct, the following items are prohibited within DO/bureau facilities:

- Illegal drugs, paraphernalia, and contraband;
- Weapons of any type, with the exception of weapons issued to law enforcement and guard force personnel for the performance of official duties. Prohibited weapons include, but are not limited to, firearms, knives or other devices with blades in excess of 4 inches, swords, explosives, incendiary devices, nightsticks, brass-knuckles, throwing stars, etc. This prohibition also includes ceremonial and/or replica weapons; and,
- Tear gas, chemical agents, and other hazardous substances. Personal protection devices, such as mace, may be permitted with specific approval of the local Treasury or bureau security office.

15. Photography Prohibited

Taking photographs within or recording images of the inside of DO/bureau facilities shall be prohibited except when specifically authorized by DO/bureau policy or on-site security officials. Examples include, but are not limited to historic or architecturally significant features and award ceremonies, celebratory or commemorative type events. Taking photographs of external features of a DO/bureau facility or other U.S. Government property which provides views or information not accessible to the public shall also be prohibited. Photography means any physical or electronically recorded image, including still photographs, x-ray images, video tapes or recordings, and motion pictures.

16. Inspection of Personal Effects

Personal effects subject to inspection are packages of all types, luggage, briefcases, attaché cases, shoulder bags, athletic bags, backpacks, and handbags. Inspection includes opening the item and viewing its contents or viewing x-ray images of the item.

a. *Entering facility.* Inspections of employee and visitor personal effects shall be conducted at entrances of Treasury facilities designated as High Impact or Critical Infrastructure and all other facilities commensurate with risk, including those

operated by contractors on behalf of DO/bureaus. The purpose of this inspection program is to deter and detect items prohibited within DO/bureau facilities. This requirement applies to all such facilities commensurate with risk.

b. *Exiting facility.* Inspections of employee and visitor personal effects shall be conducted at exits of all DO/bureau facilities designated as High Impact, all other facilities commensurate with risk, and those approved for receipt, generation, or storage of classified information. These inspections shall be conducted at periodic intervals in a systematic and impartial manner with minimal interference to official business operations. For example, exit inspections may be conducted of every fifth person exiting for a period of one hour at randomly selected hours and dates. The purpose of these inspections is to deter and detect the removal of classified materials, accountable items and/or high security items.

17. Restricted Access Area

A Restricted Access Area (RAA) established for the storage of information, information systems or assets designated as High Impact, shall be constructed in accordance with local building codes and secured in a manner that deters and detects unauthorized access.

Note: The security controls for RAAs stated here, do not satisfy the requirements for the storage of classified information or classified information systems. Construction and security requirements for facilities approved for safeguarding classified information, information systems and/or materials, are identified in Chapter V, Section 2. See also Part 17, *Storage of High-Value Assets*, below.

a. *Security.* RAAs shall be under continuous protection by guard or duty personnel with security-in-depth or shall be secured by an Intrusion Detection System (IDS) with response to alarms within 20 minutes. Security plans shall be established and maintained for all RAAs. These plans shall identify, at a minimum, officials responsible for security of the RAA, requirements for authorized access, opening and closing procedures, visitors, self-inspections and emergencies.

b. *Construction.* Walls shall be true floor to true ceiling (slab-to-slab). Doors, frames and hardware shall be of sufficient strength and materials to deter and detect unauthorized access, commensurate with the risk to the information, information systems, or assets contained within the RAA. Windows within 20 feet of the ground or otherwise readily accessible from the ground shall be secured from the inside and provided alarm coverage by motion detector. All

windows shall be covered as necessary to prevent viewing of data, assets, or operations within the RAA. Ducts and other openings greater than 96 square inches and having its smallest dimension greater than six inches, shall be provided with physical barriers of equivalent strength.

c. *Access Control.* Access control systems shall provide auditable records of access. Only high-security locks shall be used on doors to provide emergency bypass of access hardware. RAAs shall be provided with a single access point for routine access by authorized personnel. Additional access points require approval of senior DO/bureau security officials.

d. *Intrusion Detection Systems.* RAAs shall be equipped with IDS in accordance with or meeting the standards of UL 1076 or 2050. Personnel assigned to monitor alarm systems shall be the subject of a favorable trustworthiness determination. Alarm systems shall be installed such that unauthorized persons are unable to operate or observe operation of alarm control panels.

e. *Inspections.* DO/bureaus shall implement inspection programs, commensurate with the risk associated with the facility, that ensure effective functionality and effect implementation of all security equipment, systems, and procedures.

18. Storage of High-Value Assets

Storage of high-value assets, as identified by the Head of each bureau shall be stored in vaults constructed in accordance with *Federal Standard Construction Methods and Materials for Vaults* (FED STD 832), or *Federal Specification for Modular Vault Systems* (AA-V-2737). High-value assets that (a) have an immediate use for personal financial gain, (b) can be readily converted or used for any form of economic benefit, or (c) can be immediately used to produce finished securities, shall be stored in accordance with standards developed and approved by the Head of each bureau.

a. *Vault Storage Area Security.* Vaults/storage areas uses to store high-value assets shall be under continuous protection by guard or duty personnel with security-in-depth or shall be secured by an Intrusion Detection System (IDS) with response to alarms within 20 minutes. Security plans shall be established and maintained for all vaults/storage areas. These plans shall identify, at a minimum, DO/bureau officials or authorized contractors responsible for security of the vault/storage area, requirements for authorized access, opening and closing procedures, visitors entering the area, and emergencies.

b. *Intrusion Detection.* Vaults/storage areas used to store high-value assets shall be equipped with an IDS in accordance with, or meeting, the standards of UL 1076 or 2050. Personnel assigned to monitor alarm systems shall be the subject of a favorable trustworthiness determination. Alarm systems shall be installed such that unauthorized persons are unable to operate or observe operation of alarm control panels.

19. Duty, Uniformed and Guard Forces

Duty, uniformed and guard force personnel shall be the subject of a favorable trustworthiness determination based on background investigations equivalent in scope, at a minimum, to a National Agency Check and Inquiry (NACI). Duty, uniformed and guard force personnel having unescorted access to the inside of DO/bureau facilities, Restricted Access Areas, or Storage Vaults shall, at a minimum, have a the requisite background investigation to support a Secret security clearance or higher depending on the level of classified information resident within the facility or area.

20. Critical Infrastructure Physical Security

DO/bureaus shall implement the Treasury Critical Infrastructure Physical Security Program and Implementation Plan (CIPS Plan) for protecting DO/bureau critical infrastructure and key resources. DO/bureau facilities identified as critical infrastructure and those housing critical infrastructure and key resources (CIKR) shall be designated and protected at a minimum at Level IV. All critical facilities shall be assessed in accordance with the Facility Security Assessment Process identified in the CIPS Plan. All facilities designated as CIKR shall complete the CIP Asset, Function, and Services (AFS) Evaluation Questionnaire every 12 months.

DO/bureaus shall review, update, and maintain the list of DO/bureau-designated nationally critical assets on an annual basis. This process will be conducted in coordination with the review process required by TD P 85-01, Treasury Information Technology Security Program, Volume 1, Appendix B, Section 3, Critical Infrastructure Protection. This includes identifying changes to existing facilities and identifying new facilities that should receive evaluation as nationally critical. Results of annual reviews will be forwarded to the Director, OSP.

DO/bureaus shall designate a CIPS representative to the Director, OSP and provide updates within 30 days on changes to the representative's status.

Chapter V
Section 2

Standards for Security Equipment
Protecting Classified Information

Updated
3/9/12

1. Introduction

Safeguarding requirements govern the entire life-cycle of classified information from creation of an initial draft through electronic processing (including the revision process), application of required markings, printing, secure storage, handling, transmission, copying, accountability (including filing/logging and receipting), possible downgrading, declassification, release and destruction. Throughout these life-cycle stages there are procedural safeguards to augment the protection process and distinct security forms and practices that overlap the physical security, personnel security, information security and industrial security disciplines. The initial safeguarding requirements begin with authorized access to classified information by cleared employees and contractor personnel.

Classified information, regardless of its form, must be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification. Perimeter access control restrictions or the presence of uniformed guards/officers at points of ingress/egress and/or within a facility do not obviate the need for cleared employees and contractor personnel to safeguard classified information.

Treasury/bureau employees shall promptly report any suspected or actual "spills" of classified information on unclassified information systems to security officials. This is to contain the spill, prevent further contamination, and initiate the soonest and most immediate clean up activity. See Chapter III, Section 17, "Spill" Handling Procedures.

2. Responsibilities of Holders

Persons authorized access to classified information are responsible for: (1) protecting it from individuals not authorized access to it (including securing the information in approved security equipment or facilities whenever it is not under their direct control); (2) meeting safeguarding requirements prescribed by the Director, Office of Security Programs (OSP); (3) verifying the security clearance of potential recipients unknown to them and particularly co-workers or other Departmental Offices (DO)/bureau employees prior to disclosing classified information; (4) keeping classified documents under constant observation and turned face-down or covered when not in immediate use; and, (5) ensuring classified information is not communicated over unsecured voice or data

circuits, in public or private conveyances or places, overheard, or in any other manner that permits interception by unauthorized persons. Holders shall ensure classified information is only provided to those individuals authorized to receive it, and where paper copies are involved, that authorized and secure storage facilities for classified information are available and in working order. DO/bureaus may establish and publish more stringent requirements for their own use but may not lessen Treasury-wide standards for the overall protection of classified information. This includes adoption of alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements. Alternative measures shall provide protection sufficient to reasonably deter and detect loss or unauthorized disclosure. Risk management factors considered will include sensitivity, value, and crucial nature of the information; analysis of known and anticipated threats, vulnerability and countermeasure benefits versus cost.

Holders accessing Treasury Secure Data Network (TSDN) computer terminals shall follow security restrictions that include, among other requirements: (1) locking office doors housing TSDN equipment when not logged-on (including internal office doors leading to or from other TSDN equipped rooms); (2) preserving required separation between installed classified and unclassified equipment; and, (3) ensuring that unapproved equipment is not introduced within close proximity to the TSDN work station.

3. Security Equipment

The General Services Administration (GSA), in concert with Executive Branch agencies and departments originating classified information, establishes, publishes, and issues uniform national standards, specifications, qualified product lists or databases, and supply schedules for security equipment designed to provide secure storage of classified information. Whenever DO/bureaus procure new secure storage equipment is shall be in conformance with the standards/specifications established by GSA, and to the maximum extent possible, be of the type available through the Federal Supply System.

GSA-approved security containers are equipped with a built-in, dial-type, three-position, changeable, mechanical, combination lock or with an electronic lock meeting Federal Specification FF-L-2740. All intrusion detection equipment must be United Laboratories (UL) listed or equivalent as determined by DO/bureau security officials including government and proprietary equipment installed, maintained, or furnished systems.

Effective January 1, 2011, only equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA), Central Security Service at http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_EPL_02_01_AB.pdf may be utilized to destroy classified information using any method covered by an EPL. Note that equipment approved for use prior to the above date (and not found on an EPL) may be used for destroying classified information until December 31, 2016. Unless NSA determines otherwise, whenever an EPL is revised, equipment removed from an EPL may be utilized for the destruction of classified information up to six years from the date of its removal from an EPL. If any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly, the unit must be taken out of service.

4. Storage

Classified information shall only be stored and used in facilities or under conditions designed to deter and detect unauthorized access to the information.

a. Store Top Secret information by one of the following methods:

(1) In a GSA-approved security container with one of the following supplemental controls:

- Secret-level cleared guard/duty personnel shall inspect the security container once every two hours.
- An Intrusion Detection System (IDS) with responders arriving within 15 minutes of the alarm annunciation.
- Security-in-depth when the GSA-approved security container is equipped with a lock meeting Federal Specification FF-L-2740.
- In either of the following: An open storage area (secure room) or vault which is equipped with an IDS with responders arriving within 15 minutes of the alarm annunciation if the area is covered by security-in-depth or a five-minute alarm response if it is not.

(2) In a vault built to Federal Standard 832 with one of the above supplemental controls.

b. Store Secret information by one of the following methods:

(1) In the same manner prescribed for Top Secret or **until October 1, 2012**, in a bar-lock cabinet equipped with a steel lock-bar and padlock approved by the Director, OSP. After October 1, 2012, bar-lock cabinets may NO longer be used for classified information.

(2) In a GSA-approved security container or a vault built to Federal Standard 832 without supplemental controls.

(3) Security-in-Depth when a non-GSA-approved container or open storage area is used. In an open storage area (secure room) one of the following supplemental controls is required:

- Secret-level cleared guard/duty personnel shall inspect the area or GSA-approved container once every four hours.
- An Intrusion Detection System (IDS) with responders arriving within 30 minutes of alarm annunciation.

c. Store Confidential information in the same manner prescribed for Top Secret or Secret except that supplemental controls are not required.

5. Destruction of Classified/Sensitive Information and Burn-bags in the Departmental Offices

DO offices shall place all sensitive and collateral classified information (Secret and Confidential) for destruction inside "burn-bags" with alternating red/white diagonal stripes on the outside. Burn-bags are available for purchase either directly from GSA or the "Paperclips" store in the sub-basement level of the Treasury Annex. The Office of Security Programs does NOT stock or furnish burn-bags for individual offices; DO offices are responsible for maintaining their own supply of burn-bags for sensitive and/or classified paper waste.

Burn-bags must not contain ANY metal items; such as hardened steel binder clips and paper clips, keys, chains, coins/tokens, or non-metal organic waste, leftover snacks, chewing gum, materials such as crossword/Sudoku puzzles, magazines/comics, newspaper clippings, candy bar wrappers, tissues or spiral bindings and plastic tabs or heavy-duty plastics. These items will damage the cutting blades, shorten the life-cycle

and damage the DO's shredder equipment. These types of items must also NOT be placed in grey bins used for temporary storage of sensitive information awaiting collection/destruction.

Burn-bags containing ONLY sensitive information shall be labeled with the marking "SBU" on the outside of each bag. This is to distinguish it from bags containing Secret and/or Confidential classified information. DO offices are permitted to include sensitive information within a burn-bag containing classified information; however, they are responsible for securing such burn-bags in a GSA-approved security container until collected for destruction. DO offices must also put their room number on the outside of each burn-bag in the event information about particular bags needs to be tracked back to the originating office.

6. Open-Storage Area Requirements

An open-storage area is a security-approved work area or room specifically designed and configured for protecting classified information, albeit not physically stored in a GSA-approved security container. Open-storage areas may only be approved up to the Secret level. The Director, OSP approves open-storage areas in DO; bureau security officers shall approve open-storage within their bureau. If Top Secret information is required to be kept in the same area for logistical, operational or organizational needs, that information must be secured in a GSA-approved security container within the open storage area including use of supplemental controls. All other safeguards for protecting classified information apply within any DO/bureau security-approved open storage area.

a. *Construction.* Perimeter walls, floors and ceiling will be permanently and jointly constructed to provide an attached, united, whole unit. All construction must be performed in such manner to leave visual evidence of any unauthorized penetration of the area prior.

b. *Doors.* All doors shall be constructed of solid wood, metal or other solid material. New entrance doors shall be secured with a built-in GSA-approved lock meeting Federal Specification FF-L-2740 for protecting classified information. Mechanical three-position, dial-type, changeable, combination locks may continue to be used. If the latter lock fails and cannot be repaired it shall be replaced with a GSA-approved lock meeting FF-L-2740. Doors other than those secured with the aforementioned locks shall be secured from the inside with

deadbolt emergency egress hardware, or a deadbolt, or a solid wood or metal bar extending across the width of the door, or by other means approved by the Director, OSP or bureau security officer.

c. *Vents, Ducts, and Miscellaneous Openings.* All vents, ducts, and similar openings in excess of 96 square inches (and over six inches in the smallest dimension) entering or passing through an open storage area shall be protected with either bars, expanded metal grills, commercially available metal sound baffles, or an IDS.

d. *Windows.* All windows reasonably affording visual observation of classified information or activities within a facility shall be equipped with blinds, drapes, or other coverings or made opaque to obscure the ability to view inside. Windows at or within 18 feet of ground level will be constructed from or covered with materials providing from forced entry. Protection offered by windows shall be at least as sturdy as the contiguous wall construction. Open storage areas located inside a controlled compound or the equivalent may eliminate forced entry protection provided the windows are made inoperable by being permanently sealed or being equipped on the inside with a locking mechanism. Notwithstanding how the windows are modified, they must be monitored either independently or by motion detection sensors within the area by an IDS.

7. Supplemental Controls

The need for supplemental controls shall be examined by DO/bureau security officials (in conjunction with the Federal Protective Service's (FPS's) assessments of GSA-controlled/leased space). Supplemental controls shall be required in commercially leased facilities and contractor-operated facilities, on a case-by-case basis. Several determining factors include the space configuration, contiguous and neighboring structures or offices, and occupation by non-Federal Government tenants, etc. The presence of uniformed or armed officials at any DO/bureau facility (including those with existing security-in-depth provisions) does not obviate the need for individual employees and contractor personnel to maintain first-line control and protection of classified information entrusted to them.

Supplemental controls are not required in the Main Treasury Building, the Treasury Annex, the Bureau of Engraving and Printing (BEP) Headquarters, the BEP Western Currency Facility, the United States Mint headquarters, or the Denver, Philadelphia and San Francisco Mints. Each of these facilities has sufficient security-in-depth provisions already in effect for safeguarding classified information.

8. Overseas Storage

Overseas Storage. Overseas storage of classified information in diplomatic posts and facilities abroad shall be as prescribed by the Department of State via the Overseas Security Policy Board (OSPB) review process. Treasury is represented on the OSPB by OSP which consults with affected DO/bureau components and to represent the Department's concerns.

9. Repairing GSA-approved Security Containers

Repairing GSA-approved Security Containers Neutralization of lockouts or repairs of any damage affecting the integrity of a GSA-approved security container storing classified information shall only be performed by authorized and continuously escorted personnel specifically trained in the approved repair/maintenance methods The DO/bureau custodian of the information (or alternate) or an office/bureau security officer shall be present during the drilling and repair work When locked-out containers are opened in a manner causing damage to, or reducing the container's security, and thereby rendering the container no longer authorized to store classified information, the "GSA-approved" label will be removed.

Proper opening and timely repairs will allow the GSA-approved label to remain on the security container and be used to store classified information. Service and repair work distinct from changing the combination must be logged using Optional Form 89, *Security Container Records Form*, to preserve a record of the container's maintenance history. The outside of the drawer head or control drawer must also be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface. A container is considered restored to its original state of security provided all damaged or altered parts are replaced with new or cannibalized parts and any drill hole(s) repaired under Federal Standard 809B, *Neutralization and Repair of GSA-Approved Containers and Vault Doors*, dated January 1, 2010. Repainting may only be done to replicate the original (black, grey or parchment/tan) exterior color that came with the particular security container. Employees are not authorized to attach or affix stickers or decorative type labels to the outside parts of security container storing classified or sensitive information. Only magnetic or cardboard open/closed or locked/unlocked signs and Standard Form (SF) 702, *Security Container Check Sheet* and/or its magnetic holder may be affixed to such containers.

DO/bureau security officers shall maintain records of the type and location of all security equipment storing classified information and conduct periodic inventories to ensure their records are kept current. Support for conducting the actual inventory shall be provided by cleared staff within the office using such equipment.

10. Bar-lock Cabinets

Bar-lock Cabinets. Bar-lock cabinets are required to be phased out for storing Secret and Confidential information by DO/bureaus to meet the October 1, 2012 deadline in I SOO Directive 1, dated June 28, 2010. No new modifications of filing cabinets to bar-lock type (for classified storage) are permitted without written approval from the Director, OSP. Any request for a temporary exemption must include the designated DO/bureau security officer's written description of supplementary controls deemed necessary to restrict unauthorized access to the area where the bar-lock cabinet is stored along with the anticipated time-frame warranted exception.

11. Relocating Active Equipment

Security containers (and bar-lock cabinets) storing classified information shall not be relocated within, between or removed from DO/bureau occupied space without prior notification to the DO/bureau security officer. This is to enable security officials to maintain the location of such equipment and keep associated inventory and records of security combinations current.

12. Out-of-Service Equipment

Out-of-Service Security Equipment. Out-of-service security equipment shall be inspected by an appropriately cleared employee in the office relinquishing the security container. This is to ensure that no classified (or sensitive) information remains within the security container. Before security equipment is placed "out-of-service" DO/bureau security officials shall arrange for the combination to be reset to standard (or factory) combination 50-25-50. The factory combination may then be posted on the outside of the container for storage pending its excision from inventory or storage until its reuse.

The DO/bureau security officer shall certify in writing to property management, or equivalent facilities personnel, that the container is empty and authorized for removal. Equipment shall not be physically removed from DO/bureau premises unless such authorization for removal is obtained from the appropriate security officials. This notification requirement includes relocation of security equipment within an existing DO/bureau owned or leased facility.

Equipment containing classified information being relocated as part of an office move (or renovation) shall be accompanied by appropriately cleared employees to ensure the equipment and its contents are not subject to unauthorized access. Employees must also immediately report any defects, damage, or malfunctioning locks and equipment storing classified information to DO/bureau security officials for appropriate action.

13. Equipment Safeguarding Sensitive Information

National standards for safeguarding Confidential classified information may also be adapted to suit sensitive but unclassified (SBU) information storage and destruction where such application is needed to provide minimal security control.

14. Keys and Key-operated Locks

Keys and Key-operated Locks. Keys and key-operated locks may be approved by the Director, OSP, under special circumstances for storage of Secret and Confidential information but only if effective administrative procedures are established for the control and accountability of such keys and locks. DO/bureau security officials shall establish administrative procedures for control and accountability of keys and key-operated, high-security padlocks. The level of protection shall be equivalent to that afforded information being protected by the padlock.

Chapter V Section 3 — **Instructions for Changing Combinations on Security Equipment** — Updated 6/17/11

1. Introduction

This section identifies procedures for changing combinations on specific hand/key-changeable mechanical locks and electronic locks. These procedures apply to changing combinations on Mosler (MR 302) Hand Change Locks, S&G (8400/8500 Series) Key Change Locks, and electronic locks that meet Federal Specification FF-L-2740.

2. General Instructions

Combinations shall be set on either a "high-low-high" or "low-high-low basis," for example, 67-18-59 or 18-59-27. Combinations shall not be set in ascending or descending order, for example, 10-20-30 or 65-45-25. Requirements for protecting, updating, sharing, recording combinations, and reporting defective or malfunctioning equipment are contained in Treasury Security Manual Chapter V, Section 4.

3. Instructions for Mosler (MR 302) Hand Change Locks

a. Dial open the security container and put it in the "LOCKED OPEN" position. Remove the protective cover and plate(s) at the back of the lock with the proper type of screwdriver. Retract the side bolts by depressing the handle and simultaneously pushing in the triangular spring latch on the left side of the control drawer. The control drawer is the one with the dial. Remove the back cover of the lock and place it on a flat surface with the wheel-pack facing up. Slide the circular retaining clip off the top of the wheel post. Place the clip aside. Line up all parts of the wheel-pack in the order they are removed; parts assemblies are NOT interchangeable.

b. Remove the top wheel and the first spacing washer. Remove the middle wheel and the second spacing washer. Remove the bottom wheel. Leave the tension washer(s) on the wheel post.

c. Each wheel consists of two sets of rings, an inner, grey, sturdy plastic and outer metal one. Apply gentle pressure to separate the rings. Set the first number of the new combination on the bottom wheel (last wheel removed) by lining up the notch on the inner part of the wheel with the desired number on the outer part of the wheel.

Note: **NUMBERS READ COUNTER-CLOCKWISE** and combinations need to be set accordingly to avoid unintentionally setting a different combination.

Note: Inner part of the wheel has no lug on the back of it and the outer part has the gate at "0."

Place the bottom wheel back on the post. Place a washer onto the post and over the bottom wheel.

d. Set the second number of the new combination on the middle wheel.

Note: The inner part of the wheel has a lug and the outer part has the gate at "50."

Place the remaining washer onto the post and over the middle wheel.

e. Set the third number of the new combination on the last (or top) wheel.

Note: The inner part of the wheel has a lug and the outer part has the gate at "0."

Slide the retaining clip back onto the top of the post. Set the dial at "50."

f. Replace the back cover. Do NOT immediately lock the container but test the new combination with the control drawer remaining in the open position.

- If it works, try it a few times before closing and locking the container until satisfied the new combination works;
- Update Standard Form (SF), 700 *Security Container Information* and make sure it is securely transported to the office/bureau security officer or designated and cleared administrative person responsible for maintaining records of combinations to security equipment; and
- If it does not work, repeat the previous steps.

Note: **Most hand change combinations that do not work are the result of combinations being set clockwise as opposed to counter-clockwise.**

g. If the new combination still does not work after resetting, immediately contact office/bureau security officials and/or an authorized locksmith. Do not leave an open security container storing classified information without an appropriately cleared person present. In extreme circumstances, classified holdings must be transferred to alternate secure storage if the container is not lockable.

4. Instructions for S&G (8400/8500 Series) Key Change Locks

a. Put the container in the "LOCKED OPEN" position. Remove the protective cover and plates at the back of the lock. Retract the bolt by depressing the handle and simultaneously pushing in the triangular spring latch on the left side of the control drawer. Do not remove the back of the lock. Cover the vertical (12 o'clock) opening index line on the front dial with thumb or piece of tape. Dial the present combination onto the change index line (to the left of the opening index). Use the normal dialing sequence, but stop dialing when reaching the third number of the combination. Do not turn the dial to "0."

b. Insert the long end of the change key into the change-key hole in the back of the lock. The key must be a 6720 change key. Insert the key according to the shape of the key-hole. Do **NOT** force it; the key should insert easily into the back of the lock. Turn the key one-quarter turn counter-clockwise. Leave the key in place, do **NOT** remove it.

c. Dial the new combination using the change index line as a guide. Use the normal dialing sequence. Stop when coming to the third combination number. Do **NOT** turn the dial to "0."

Note: If an error has been made during the combination setting process, restart the dialing sequence again from the beginning.

d. Turn the key one-quarter turn clockwise and remove it. Do **NOT** lock the container but test the new combination with the control drawer in the open position.

- If it works, try the combination a few more times before closing and locking the container when satisfied the new combination works;
- Update SF 700, *Security Container Information*, and make sure it is securely transported to the office/bureau security officer or administrative person responsible for maintaining records of combinations to security equipment; and,

- If it does not work, immediately contact your office/bureau security officer and/or an authorized locksmith, as appropriate. Do **NOT** leave an open security container storing classified information without an appropriately cleared person present.

5. Instructions for Electronic Locks Meeting Federal Specification FF-L-2740

a. Dial open the X-07, X-08, or X-09 equipped lock on the security container using the existing combination. Retract the bolt by depressing the handle and simultaneously pushing in the triangular spring latch on the left side of the control drawer. Remove the protective over and plates at the back of the lock.

b. Insert the two-prong change key; this is a different type of change key from those on mechanical locks and comes with all new electronic locks on security containers. Rotate the dial to the left. The "key" symbol will appear in the top right corner of the liquid crystal diode (LCD) readout. Dial the current combination. If the current combination is unknown, the serial number printed on the inside lock cover can be used.

Note: To read the serial number printed on the inside lock cover requires removal and replacement of the back cover.

c. Rotate the dial slowly to the right until "SL" (Select Mode of Operation) appears on the LCD readout. Rotate the dial to the left. Stop on "1," "2," or "3," to select the desired mode of operation.

Note: "1" refers to single combination mode, "2" refers to dual combination mode, and "3" refers to supervisory/subordinate mode.

d. When mode "1" has been selected, reverse direction by dialing to the right until "EC" (Enter Combination) appears. If mode "2" or "3" has been selected, the LCD readout will be "E1" (Enter First Combination). Depending on the selected mode, continue with the steps to change the combination, in the following manner.

(1) *Single Combination Mode.* Dial in the new combination after "EC" appears. Rotate the dial slowly to the right. The new combination numbers will flash three times on the LCD readout until "PO" (Pull Out Change Key) appears. Remove the change key and "CC" (Confirm Combination) appears. Dial in the new combination to confirm the change. "OP" (Open) will appear. Rotate the dial to the right and retract the bolt. The new combination is now set.

(2) *Dual Combination Mode.* Dial in the first new combination after "E1" appears. The first new combination numbers will flash three times on the LCD readout, then "E2" (Enter Second Combination) will appear. Dial in the second combination. The second new combination will flash three times, and then "PO" will appear. Remove the change key and "CC" appears. Dial in the new combinations to confirm the changes. "OP" will appear. Rotate the dial to the right and retract the bolt. The new combinations are now set.

(3) *Supervisory/Subordinate Mode.* When the "E1" symbol appears on the LCD readout, enter the supervisory combination. When the "E2" symbol appears, enter the subordinate combination. When "CC" appears, remove the change key. Confirm the new combinations in the same manner as in *Dual Combination Mode.*

6. Notes Concerning Electronic Lock Combination Changes

a. If the new combination is not what is desired, pull out the change key while the new numbers are still flashing on the LCD readout. "EC," "E1," or "E2" will reappear in successive order. Reinsert the change key and rotate the dial to the left. The "key" symbol will reappear. Dial in the new combination(s) and resume the rest of the changing procedures.

b. If the "key" symbol and "lightning bolt" appear together, stop, and rotate the dial to the left. The "key" symbol will appear. Dial in the current combination and continue with the changing procedures.

c. If the "lightning bolt" appears while confirming combinations, stop, and insert the change key. Rotate the dial to the left until the "key" symbol appears. Dial in the current combination and continue with the changing procedures.

d. If the combination is misdialed or the change is not completed, **the lock automatically reverts back to the immediately preceding combination(s).** If this happens, repeat the changing process. The old combination remains valid until new combination(s) are confirmed.

Note: As an added precaution, after the new combination(s) are set and confirmed, record the new combination(s) numbers and test them before closing and locking the container.

e. Electronic locks (X-07, X-08, and X-09) meeting Federal Specification FF-L 2740 vary in the direction in which they are dialed open. X-07 locks are no longer manufactured, but replacement parts are still available and such locks may continue to be used.

- X-07 locks dial left/right/left, similar to mechanical locks.
- X-08 locks dial in a single direction, unlike mechanical locks.
- X-09 locks dial like X-07 locks do.

Chapter V
Section 4

Updating and Recording Security Combinations

Updated
6/17/11

1. Introduction

This section identifies time frames and requirements for updating and recording combinations on security containers and equipment protecting classified information. This also includes instructions on reporting damaged, defective, malfunctioning equipment and procedural requirements before excess equipment is surplused. These procedures shall also be used for security equipment safeguarding sensitive but unclassified information.

2. Background

Only employees or contractor personnel, with the appropriate security clearance, shall change combinations to built-in, three-position, dial-type, hand/key changeable mechanical combination locks and electronic locks (meeting Federal Specification FF-L-2740) on security equipment protecting classified information. Cleared U.S. Government employees working for another Federal agency or department may be relied upon to change combinations, for example an available U.S. Secret Service employee within the same or adjoining Federal or commercial office building.

In lieu of appropriately cleared persons, Departmental Offices/bureaus may designate specific employees or use contractor personnel (with the expertise) to change security combinations on equipment protecting sensitive information. However, they must ensure specific employees or contractor personnel do **NOT** record or otherwise retain the new combination and do **NOT** have unauthorized access to the security equipment or space where the equipment is located.

3. Time Frame Requirements

Combinations shall be updated under any of the following conditions:

- When the security equipment (including previously surplused equipment) is first placed into service with the end-user;
- When a person knowing the combination no longer requires access to it (unless existing controls prevent the person's unauthorized access to the security equipment as in a Sensitive Compartmented Information Facility (SCIF) or other

secure area with prescribed access control restrictions);

- When a combination has been subjected to possible compromise, actual compromise, or unauthorized disclosure;
- When the equipment is taken out-of-service; and,
- At least every three years, unless conditions dictate sooner, such as the need to store a particular type of classified information or material. This minimum time frame is to ensure combinations have an official termination point requiring updating. It is also to keep combinations to infrequently opened security equipment accounted for and to avoid the combination being lost or forgotten.

4. Damaged, Defective or Malfunctioning Equipment

Users must report any damaged, defective or malfunctioning security equipment protecting classified or sensitive information to DO/bureau security officials for prompt action. A report could be triggered by any instance wherein the dial doesn't "feel" right to the user or there is discernable damage/defect. Examples include, but are not necessarily limited to the following:

- The dial or handle turns too loosely, tightly/stiff or "catches" when turned.
- The dial "wobbles" when turned or comes off.
- The electronic LCD digits do not display, blink on/off or only partially display (numbers show up only on the top half or bottom half of the digital readout).
- The numbers have to be dialed one or more notches higher/lower than the set combination on mechanical locks.
- One or more container drawers "stick/catch" and/or do not fully open or metallically "squeak" (lacking lubrication or are misaligned).
- Containers require forceful effort to shut or drawers need to be "lifted" and/or "pushed" to close and lock.

Users must notify security officials as soon as possible with respect to any problem with the equipment to avoid potential lock outs and/or costly manual drilling and attendant repairs.

5. Out-of-Service and Surplused Equipment

Security equipment used for classified information taken out of service must be inspected by appropriately cleared personnel in the office directly relinquishing the equipment. All classified and sensitive information must be removed and placed in alternate secure storage. If classified or sensitive information is being disposed of, the material must be placed in burn bags. Classified information in burn bags for disposal must be secured until collected for destruction.

When security equipment is excessed as part of an office move, sensitive information for destruction must **NOT** be abandoned by office occupants. The office giving up the security equipment is responsible for notifying appropriate security personnel so the sensitive information may be properly disposed. No security equipment shall be placed into excess inventory or surplused unless it has been emptied by the office relinquishing it and inspected by DO/bureau security officials.

Combination locks on security equipment taken out of service shall be reset to the factory combination of 50-25-50 or 10-20-30 and the equipment so labeled on the exterior surface. Except for out-of-service and surplused equipment, combinations shall never be identified on the outside of a security container.

6. Recording Combinations

a. *Forms.* Combinations on security equipment shall be officially recorded on Standard Form (SF) 700, *Security Container Information.* Completed SF 700 forms recording combinations protecting classified information shall be centrally (or locally) stored and filed for ease of access by authorized security or designated administrative personnel with the appropriate security clearance. Protection provided to each completed SF 700 form shall be in the same manner as the highest level of classified information being safeguarded from the time the form is completed to receipt by DO/bureau security or cleared, designated administrative officials for filing.

b. *Procedures.* DO/bureaus are responsible for obtaining and maintaining their own supply of SF 700 forms. Recording of combinations shall not be included in numerical totals of classified documents generated and annually reported to Treasury's Office of Security Programs (OSP).

c. *Accounting.* DO/bureau security officials shall conduct periodic surveys to ensure security containers are physically located where records on file indicate. Surveys shall also ensure that recorded combinations, particularly on infrequently opened security containers, are what actually unlock the equipment to avoid loss of the combination. Office occupants responsible for particular security containers shall

assist security officials in these surveys including updating SF 700 forms to reflect changed information. Supervisors shall ensure that departing employees turn over the combination(s) to appropriately cleared back-up personnel in transferring responsibility for classified and/or sensitive records. This is also to avoid loss of combinations and attendant drilling/repair costs.

7. Sharing Security Combinations

An individual's security clearance level shall be verified (through personnel security channels and/or their office's security point of contact) and their need-to-know authorized by their supervisor before providing any security combination to another individual. Security container/safe custodians shall ensure the new person's name is added to an updated SF 700. This information shall be relayed to the DO/bureau security or administrative official responsible for maintaining security combination records.

Completed SF 700 forms must be transported in the same manner as the highest level of classified information contained in the security container or equipment. For example, SCI/SAP and Top Secret combinations on SF 700 must be hand-carried; Secret and Confidential combinations may be hand-carried or sent via double-wrapped envelopes through the organizations internal mail delivery system.

Chapter V Section 5 **Credentials, Badges/Shields and the Law Enforcement Officers Safety Act** Updated 5/16/14

1. Introduction

The purpose of this section is to implement policy and identify requirements for issuing, using, controlling, and accounting for official credentials and badges/shields authorized for use by Departmental Offices (DO)/bureau employees. This section also addresses the Law Enforcement Officers Safety Act of 2004 (Public Law 108-277), hereafter the "LEOS Act". Any employee who violates this policy with respect to the use, abuse or misrepresentation for other than conducting official U.S. Government business will be subject to administrative and/or disciplinary action.

This section covers four areas: information about and authorizing use of credentials and/or badges/shields for current and retired employees; the contents of credentials and badges/shields; issuing, maintaining, and transmitting credentials and the LEOS Act.

2. Background

Credentials and badges/shields are issued for and authorized to be used only to conduct official United States Department of the Treasury business with the public or Federal, State, local, Tribal, or foreign officials, as authorized by law, statute or Treasury/bureau regulation or policy. Credentials identify the DO/bureau employee by name and official position. Badges/shields are metallic emblems that may in some cases accompany the credential.

3. DO/Bureau Responsibilities

The Director, Office of Security Programs (OSP) has overall responsibility for developing Treasury-wide policy to efficiently manage and control the design, authorization, issuance, and accountability of DO/bureau credentials and badges/shields.

Bureau heads/authorized DO offices shall establish written procedures for issuing credentials (with or without badges/shields) to authorized employees within their organization. This includes identifying an issuing authority either within the security structure or administrative component of the DO/bureau along with attendant funding and resources. Heads of bureaus, authorized DO offices (Assistant Secretary or Director level), the Director, OSP, the Inspector General (OIG), the Treasury Inspector General for Tax Administration (TIGTA), and the Special Inspector General for the Troubled

Asset Relief Program (SIGTARP) will approve its written policy and shall ensure the following actions are performed:

- Identify responsibilities and adequate funding for: (1) issuing, controlling, and maintaining stocks; and, (2) accounting for, canceling, and destroying credentials and badges/shields.
- Identify and assign responsibility to a designated security or administrative official.
- The designated DO/bureau security or administrative official shall maintain appropriate accountability records; including records about issued, returned, lost, stolen, canceled, awarded and destroyed credentials and badges/shields.
- Ensure that all credentials and badges/shields accurately represent the official position and duties of the bearer.
- The loss or theft of credentials and badges/shields shall be immediately reported to designated DO/bureau security officials or administrative officials.
- Design and sample credentials are provided in advance to the Director, OSP, who may require changes for accuracy and consistency with this section. Following the Director, OSP review, the heads of bureaus and authorized DO offices (Assistant Secretary or Director levels) must approve badge/shield designs within their own DO/bureau.
- Periodic inventories of existing stock of blank credentials, badges/shields and cases/folders are conducted. Inventories shall also be conducted prior to transfer of responsibility from one designated DO/bureau issuing authority to a successor.
- All persons issued credentials and badges/shields receive mandatory training on the requirements and obligations governing such use under DO/bureau policy and prescribed professional standards of conduct.

4. Recognition

Credentials shall generally be accepted in verifying the bearer's identity at DO/bureau-owned, leased, or operated facilities to conduct official business. However, possession of credentials does not relieve the bearer from complying with established access control requirements for employees, contractors, visitors, or other U.S. Government agencies, State, local, Tribal, or municipal authority. Circumstances casting reasonable doubt on

the authenticity or validity of the credential or the matching identity or authority of the bearer shall be reported to appropriate DO/bureau security officials.

5. Use as Awards for Retiring Employees

Credentials may be canceled and awarded (along with badges/shields) to departing employees when such awards are established and approved through a DO/bureau employee incentive award program. Cancelled credentials shall be either perforated or permanently stamped to reflect that the individual is "retired" or otherwise indicate the credential is awarded "for honorable service." Cancelled credentials and badges/shields must be marked in a manner distinct from active credentials, e.g., encased in Lucite, fitted with a "retired" or "honorable service" plate or other (shadow-box) display-type manner, as approved by the Director, OSP. Use shall be limited to display purposes only.

Issuance of new credentials to retirees or persons previously separated from Federal service or as replacement for lost, stolen or damaged awards is not authorized. Honorees shall not sell or barter cancelled credentials. The cancelled credentials shall only be held by the retired employee. Retired credentials are not intended or to be used for purposes of meeting the identification provisions of the LEOS Act. See part 20 for procedures regarding the issuance of identification cards to retiring and retired DO/bureau employees in accordance with the Act.

6. Content

Credentials shall consist of upper and lower laminated cards either permanently affixed or inserted inside a protective case or folder. The case or folder promotes durability and inhibits removal or tampering.

a. *Upper and lower laminated cards.* The upper portion of the credential shall display the printed legal name and official position title (reflecting the job series) of the bearer. The bottom portion shall generally describe the bearer's duties, his or her signature, the authenticating official's signature and bearer's photograph. At a minimum, all credentials shall include the following items:

- The bearer's full-face, color (plain, light background), true likeness in civilian attire or in the uniform the employee wears while on duty. If prescription glasses are worn full-time, these will be worn when the bearer's photograph is taken.

- The bearer's printed legal name, official position title (reflecting their job series), signature and the date of issuance.

- The term, "United States Department of the Treasury."
- The seal of the Treasury Department or bureau.
- The name of the employing bureau.
- The signature(s) of the authenticating DO/bureau official(s), as applicable.
- A designated serial or control number.
- The description of the bearer's legal, statutory, and regulatory or other specific authorized duty (ies).

b. *Use of pseudonyms.* A pseudonym is only permitted for authorized IRS employees in accordance with Public Law 105-206, *Internal Revenue Service Restructuring and Reform Act of 1998*. Whenever use of a pseudonym is permitted, the IRS must implement strict control procedures for issuing and monitoring the use of such credentials. If a pseudonym is authorized, only one credential may be issued in the pseudonym name. All such procedures shall be submitted to the Director, OSP.

7. Case or Folder

The credential carrying case or folder shall be approximately three inches in width and five inches in length when closed; individual DO/bureau sized cases or folders may vary. Cases or folders normally fold in half and may have two carrying pockets for the upper and lower portions of the credential or have the upper/lower portions permanently affixed. Cases or folders may not be used as wallets or contain other materials unrelated to official use, for example, money, business cards, courier card, etc. Cases or folders may be equipped with a carrying clip and badge/shield carrying surface at the discretion of the issuing DO/bureau component.

8. Security Clearance

Credentials shall not indicate that the bearer has a security clearance or is otherwise eligible for access to classified information. Certification of a security clearance shall be handled via established personnel security verification procedures and obtained in advance of all instances involving the need for access to classified information. For internal recognition purposes, a credential may be equipped with a DO/bureau-unique alpha-numeric code or varying background colorization to reflect the bearer's security clearance provided such indication is not apparent to casual viewers.

9. Requirements for Issuing Credentials and Badges

a. Credentials without a badge/shield may be issued to authorized DO/bureau employees who do not necessarily possess specific statutory authority but are authorized to conduct official business in accordance with existing DO/bureau regulations or policy.

b. Credentials with a badge/shield may be issued to DO/bureau employees that are explicitly authorized by statute, regulation, or existing policy to carry badges/shields by the heads of bureaus and authorized DO offices (Assistant Secretary or Director level).

c. Credentials with a badge/shield issued to individuals in positions defined as "Treasury Law Enforcement Officer" under Treasury Order 105-12 must follow prescribed training and proficiency standards for Treasury Law Enforcement Officers prior to carrying a firearm. Individuals may take equivalent training to that provided by the Federal Law Enforcement Training Center for firearms proficiency, as long as it is a recognized program by the Federal Government. Such training must be documented with the employing bureau, and will be accepted for purposes of complying with TO 105-12. Positions where the duties are limited to auditing, inspecting, legal, or other activities that do not require the DO/bureau employee to qualify with a firearm and/or wear a police-type uniform, are not authorized badges/shields.

d. Credentials shall normally be issued only to permanent DO/bureau employees upon need or request. Credentials may be issued to temporary employees when determined necessary by the heads of bureau or authorized DO office (Assistant Secretary or Director level) (on a case-by-case basis or by category of employee position). Examples include temporary hires or a Federal employee of another agency or a contractor who possesses unique skills and is engaged in authorized activities on behalf of a DO/bureau component.

e. Requests to issue credentials to employees in positions not previously identified as requiring them shall be justified in writing and approved by the Director, OSP. Prior to submitting this request to the Director, OSP, the employing DO/bureau legal counsel must review the request and particularly the specific authority to be conveyed upon the bearer. All such issuances to other than permanent employees must be supported by a written determination of need by the requesting element and evaluated by the credential issuing authority for compliance with this section.

This shall also be based on the incumbent's active engagement in activities supporting the need for credentials and/or badge/shield to fulfill official responsibilities and not just their official title.

10. Treasury Department Form (TD F 15-05.14) Request and Receipt for Official Credentials/Badges

TD F 15-05.14 (see Attachment 1) available on-line at http://thegreen.treas.gov/policies/Forms1/Request%20and%20Receipt%20for%20Official%20Credential.pdf is the vehicle for requesting and receipting for credentials. Office Director level officials are responsible for the form's completion and providing written justification as to why the perspective person should be authorized to have a DO/bureau credential. DO offices requesting credentials can be faxed, emailed or hand-delivered to the Office of Security Programs. Prior to receipt of official credentials, recipients shall also receive training on credential requirements, i.e., the issuance, official use, controlling, accounting for/safeguarding, returning, and administrative penalties for possible misuse, abuse or misrepresentation. Credential issuers shall document such training along with their records of issuance to individual employees.

11. Legal Division Employees

When the employing DO/bureau or the Legal Division requests a credential to be issued to an employee within the Legal Division, that credential shall be issued by the DO/bureau issuing authority served by the Legal Division office in which the employee is assigned. Legal Division personnel are not authorized to have badges/shields.

12. Credential Authorization

Individuals may not authorize or otherwise validate their own credentials. Authentication shall be performed by the following entities.

a. Credentials for all DO officials and the heads of bureaus shall be authenticated by the Director, OSP.

b. Heads of bureaus, the OIG, the TIGTA, the SIGTARP and the General Counsel shall authenticate credentials for personnel assigned to their respective organizations.

13. Assignment of Control Numbers

A serial or control number shall be used for accountability purposes to allow for credentials and badges/shields to be readily traced to the DO/bureau person to whom they were issued. Credentials and badges/shields shall normally be issued in consecutive order as recipients are authorized to receive them. Once assigned, the serial or control numbers shall not be reused except to ensure compliance with Federal Property Management Regulations relating to U.S. Government property or as authorized by the Heads of Bureaus and Authorized DO Offices (Assistant Secretary or Director levels).

14. Credential Updates

Credentials remain valid for the duration of the bearer's DO/bureau employment for which they are issued. Credentials may be updated and reissued to the bearer under the following conditions:

- Upon legal name change (e.g., marriage/divorce).
- Promotion or reassignment to a different position to reflect a change in the bearer's authority.
- Significant change in the bearer's appearance over time.
- Excessive wear, or lapse of sufficient time for a lost or stolen credential to be recovered, found, and/or returned.

15. Controls and Recordkeeping

All credential and badges/shields are property of the U.S. Government and the issuing DO/bureau office. Credentials, badges/shields must be immediately returned upon termination of employment, need, or upon request of the issuing authority. Credentials and badges/shields are not transferable and are subject to inventory and inspection at the discretion of the Director, OSP or issuing authority. Each recipient shall be required to sign TD F 15-05.14 when issued a credential and/or badge/shield. Costs associated with DO/bureau manufacture, procurement, safeguarding, issuance, and accountability of credentials and badges/shields shall be minimized.

DO/bureau issuing authorities shall maintain TD F 15-05.14 record on the disposition of all credentials and badges/shields. Those persons terminating employment shall return their credential and badge/shield to their DO/bureau security office or issuing authority prior to terminating employment. DO/bureau supervisors shall ensure credentials and

badges/shields are returned and accounted for prior to allowing the employee to separate from DO/bureau employment.

Credentials of persons who retire or separate from their employing DO/bureau component may be held by the issuing authority for a period of time at their discretion and then destroyed, unless approved for special disposition as part of a DO/bureau award program. Badges/shields shall also be returned to inventory unless approved for special disposition as part of a DO/bureau award program.

16. Transmittal of Credentials/Badges

Whenever credentials and badges/shields are transmitted between DO/bureau facilities, they will be packaged in double envelopes together with a transmittal memo or letter. Within the United States including the Commonwealth of Puerto Rico, U.S. territories, or possessions, credentials and badges/shields will be sent via: (1) U.S. Postal Service (USPS) registered mail or overnight express mail; or, (2) at the DO/bureau discretion, via overnight mail carrier authorized by the General Services Administration for express mailings. Within overseas areas, credentials and badges/shields will be mailed by registered mail to, from, and within the overseas areas, or couriered via diplomatic pouch, as warranted.

17. Safeguarding and Reporting Loss or Theft

a. Persons who have been authorized credentials and/or badges/shields are personally responsible for safeguarding them from loss, theft, or possible misuse by any reasonable means, while minimizing their personal risk. Credentials and badges/shields shall be carried on the bearer's person and not left or stored in a manner allowing access by unauthorized persons. When not used for a period of time, or when the bearer is on extended leave, the credential should be safeguarded, e.g., secured in an office security container or locked file cabinet.

b. The loss or theft of credentials and badges/shields must be reported to DO/bureau security officials as soon as possible, but not later than 48 hours following the loss of theft. For those bureaus with access to the National Crime Information Center (NCIC), an NCIC entry reporting the loss or theft should be made in conjunction with notification to the responsible DO/bureau security official.

c. A signed report must be submitted identifying the individual by name, credential and badge/shield number(s), date, location, and relevant facts about the loss or theft. Recovered credentials and badges/shields must be reported to the

DO/bureau issuing authority without unreasonable delay. Accountability records shall be adjusted to reflect the recovery. The recovered credential may be either destroyed or reissued to the bearer; however, individuals shall not retain more than one credential at a time, except for individuals that may be detailed to DO/bureaus and possess a credential from their employing agency.

18. Administrative or Disciplinary Action

Inappropriate use or abuse of official credentials and badges/shields will be cause for administrative or disciplinary action. Such action might include temporary suspension, reassignment, revocation of official duties and responsibilities, surrender/recall of the bearer's credential and badge/shield, dismissal, and/or other penalties. Supervisors are required to immediately confiscate an employee's credential and badge/shield upon any allegation and/or report of the circumstances of such abuse, misuse, or misrepresentation and shall notify appropriate security officials. Instances involving senior DO or bureau officials shall be reported concurrently to the Director, OSP and the Office of Inspector General (OIG), or as applicable, to the TIGTA or to the SIGTARP. The OIG or TIGTA or SIGTARP shall decide in consultation with the Director, OSP whether an investigation is warranted and what office will conduct the investigation.

19. Unauthorized Use, Misuse and Abuse

Credentials and badges/shields shall not be used for any un-official or personal business or to solicit preferential treatment from civil/police authorities; for example, acting in such manner to either impersonate, impart, state, or otherwise intend to be perceived by civil/police authorities as a bona fide Treasury Law Enforcement Officer as that term is defined in TO 105-12. Such misuse, abuse or misrepresentation will result in the immediate and permanent confiscation of the employee's credential and badge/shield. Penalties may be imposed pursuant to law for the improper use of such official identification pursuant to the following statutes:

a. 18 United States Code (USC) Section 499 states: "Whoever falsely makes, forges, counterfeits, alters or tampers with any naval, military, or official pass or permit, issued by or under the authority of the United States, or with intent to defraud uses or possesses any such pass or permit, or personates or falsely represents himself to be or not to be a person to whom such pass or permit has been duly issued, or willfully allows any other person to have or use any such

pass or permit, issued for his use alone, shall be fined under this title or imprisoned not more than five years, or both."

b. 18 USC Section 701 states: "Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department of agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both."

c. 18 USC Section 1028 establishes penalties (fines and imprisonment) for fraud and related activity in connection with identification documents.

20. Impact of the Law Enforcement Officers Safety (LEOS) Act of 2004

The LEOS Act permits the carrying of concealed firearms by qualified law enforcement officers and qualified retired law enforcement officers.

a. *Employment Requirements under the LEOS Act.* Qualified law enforcement officers are permitted to carry concealed firearms if they meet all the following requirements:

- Is an employee of a U.S. Government agency that: (1) is authorized by law to engage in or supervise the prevention, detection, investigation, prosecution, or incarceration of any person for any violation of law; **and** (2) has statutory powers of arrest.
- Is authorized by the employing agency to carry a firearm.
- Is not the subject of any disciplinary action by the agency.
- Meets standards, if any, established by the DO/bureau that require the employee to regularly quality in the use of a firearms.
- Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance.

- Is not prohibited by Federal law from receiving a firearm.

b. *Retirement Requirements under the LEOS Act.* Qualified law enforcement officers who retire in good standing for reasons other than mental instability must meet all of the following requirements:

- Was an employee of a U.S. Government agency that: (1) is authorized by law to engage in or supervise the prevention, detection, investigation, prosecution, or incarceration of any person for any violation of law; **and** (2) had statutory powers of arrest;

- Was regularly employed as a law enforcement officer for an aggregate of 15 years or more; or (2) retired from service with a DO/bureau, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by the employing DO/bureau component.

- Have a non-forfeitable right to benefits under the DO/bureau retirement plan.

- During the most recent 12-month period, have met, at the expense of the retiree, his/her primary State of residence's standards for training and qualification for active law enforcement officers to carry firearms.

- Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance. The employee must meet his/her state of residence standards, if any, regarding alcohol or drug use by law enforcement officers authorized to carry a firearm as part of the annual certification requirement.

- Is not prohibited by Federal law from receiving a firearm.

c. *Required Photographic Identification under the LEOS Act.* Qualified law enforcement officers and qualified retired law enforcement officers are required by the Act to carry photographic identification issued by the U.S. Government agency for which the individual is employed as a law enforcement officer or from which the individual retired from service as a law enforcement officer. Additionally, qualified retired law enforcement officer are required to obtain certification issued by the state he/she primarily resides that indicates that the individual has, within the last year, been tested or otherwise found by that state to

meet the standards established by the state for training and qualification for active law enforcement officers to carry a firearm.

21. Additional Identification Requirements/Procedures

a. *Qualified Retired Law Enforcement Officer Identification.* DO/bureaus may design and issue photographic identification for qualified retired (retiring) law enforcement officers in good standing. Such designs shall be reviewed and approved by the Director, OSP. Specific wording on the type of DO/bureau identification, attesting to the qualification of the retired law enforcement officer, shall be reviewed and approved by the Legal Division of the DO/bureau from which the employee is separating. The receipt by a qualified retired law enforcement officer of an identification card does not grant the bearer any legal, statutory, regulatory or other authority. Retired Law Enforcement Officer Identification shall not be issued to employees whose:

- Retirement was a result of any determination to remove or proposal to remove the employee from Federal employment.
- Retirement was a result of a psychological fitness for duty evaluation, whether resolved or unresolved, prior to retirement.
- Retirement was a result of suspension or revocation of the employee's security clearance.

b. *Qualified Retired Law Enforcement Officer Responsibility.* Qualified retired law enforcement officers (not DO or its bureaus) are responsible for ensuring that they meet all requirements of the LEOS Act. DO/bureau components shall not train or qualify retired employees to carry a firearm, as authorized under the Act.

c. *Replacing Identification.* Replacement of qualified retired law enforcement officers' identification is authorized only where the former employee: (1) substantiates in writing that his or her previously-issued qualified retired law enforcement officer identification has been lost, stolen, or destroyed; (2) provides a copy of the police report attesting to such loss or theft; and (3) includes a notarized copy of their primary State of residence's certification that they have, not less recently than one year before the date the individual intends to carry a concealed firearm, been tested or otherwise found by the state to meet standards established by the state for training and qualification for active law enforcement officers to carry a firearm of the same type as the concealed firearm. Costs for

replacing lost or stolen qualified retired law enforcement officer identification may be charged, at the discretion of the former DO/bureau, to the retired employee.

d. *Former Treasury/Bureau Law Enforcement Officers Identification.* Former qualified law enforcement officers previously employed by the Bureau of Alcohol, Tobacco and Firearms (ATF); the U.S. Customs Service (Customs); the U.S. Secret Service (USSS); or the Federal Law Enforcement Training Center (FLETC), when those bureaus were part of the Department of the Treasury, shall obtain qualified retired law enforcement officer identification, under the LEOS Act, from the Department of Justice (DOJ) for ATF, or the Department of Homeland Security (DHS) for Customs, USSS, and FLETC, in compliance with procedures implemented by those departments.

e. DO/*bureau credential issuing authorities.* Upon receiving a request for an identification card by a retired/retiring qualified law enforcement officer, the DO/bureau issuing authority shall run sufficient checks on the employee to determine: (1) if there (is/was) any action initiated to remove or to propose to remove the officer from service at the time of retirement, (2) whether or not the officer is considered to have retired or is retiring "in good standing," (3) if there (is/was) any proposal to suspend or revoke the officer's security clearance at the time of retirement, and/or (4) if the officer retired or is retiring under a pending psychological fitness-for-duty inquiry, or after being found not fit for duty. Upon a determination that the individual retired or retiring in good standing, the retired identification may be issued in accordance with this section.

It shall be within the discretion of the employing DO/bureau to issue a retired law enforcement officer credential. Should the DO/bureau component (1) make a finding that the subject is not qualified; or (2) enter into an agreement in which the subject agrees that he or she is not qualified, the subject shall not be issued a retired law enforcement officer credential or identification card.

Attachment 1

Department of the Treasury
Request and Receipt for Official Credentials

(Employee Name: _____ Date of Birth: _____

SSN: _____ Job Title on Credential: _____

Justification for Official Credentials (description):

Signature of Office Director: _____

In acknowledging receipt of official Department of the Treasury/bureau credentials, agree to surrender them to the Treasury/bureau issuing authority for accountability and appropriate voiding prior to the termination of my employment in the position in which they were duly authorized. I have been advised that these credentials are only for the conduct of official Treasury/bureau business and that use for non-official or personal reasons may constitute rationale for administrative action.

I have been further advised to immediately report the loss, theft or misplacement of these credentials to the Treasury/bureau issuing authority.

Assigned Control Number _____

Employee's Signature _____ Date of Issue: _____

Issuing Authority: _____

Notice: The information requested is protected by the Privacy Act, 5 U.S.C. 552a which requires that Federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that the authority for soliciting your Social Security Number (SSN) is Executive Order 9397 which authorizes agencies to solicit SSNs for use as identifiers for administrative purposes. This form will be used as a means to prepare and issue a credential. Providing the information requested, including the SSN, is voluntary; however, if some or any part of the requested information is not provided, the effect will be that you will not be issued a credential.

TD F 15-05.14 (4/08)

Chapter V Section 6 **Issuance of Courier Card/Letter based on Demonstrated and Recurring Need** Updated 3/31/14

1. Introduction

Electronic transmission of classified information over secure communications (e.g., via secure e-mail) is preferable to physical transfer of hard copy documents. Hand-carrying classified information shall be minimized to the greatest extent possible and authorized only when the information is not available at the destination, and operational necessity, or a contractual obligation requires it, or the information cannot be sent via a secure e-mail/facsimile transmission or other secure means. This section establishes standards for the issuance and use of courier cards/ letters to Departmental Offices (DO)/bureau employees and contractor personnel when secure electronic transmission is either unavailable or impractical.

Courier cards/letters may substantiate the bearer's authorization to transport classified national security information (and sensitive compartmented information (SCI) or special access program (SAP) material as may be approved by Treasury's Special Security Office (SSO)). Courier cards/letters may be issued to authorized employees or contractor personnel to hand-carry and/or to transport classified information between DO and Treasury bureaus and other U.S. Government agencies or departments ***based only on a demonstrated and recurring need***. All authorized employees or contractors must have the appropriate security clearance at the same level (or higher) than the classified information entrusted to them for safekeeping and receive appropriate training in conjunction with being issued a courier card.

2. Couriers

An employee or contractor personnel whose work entails the demonstrated and recurring responsibility for physically transporting and securely delivering classified information between DO and Treasury bureaus and/or to other Federal agencies, instrumentalities, or their cleared contractor personnel, or other authorized parties.

3. Courier Approval

Requests for courier cards shall identify the demonstrated and recurring need ***in terms of measurable frequency.*** Within DO/bureaus, designated couriers for collateral classified information that are approved will be issued a courier card by the Director, Office of Security Programs (OSP). IRS' Criminal Investigations Division (IRS-CI) and the Financial Crimes Enforcement Network's (FinCEN) security liaison with OSP have been

authorized by the Director, OSP to issue collateral courier cards to their designated employees and contractor personnel with a demonstrated and recurring need. The decision to authorize other bureaus to issue Treasury courier cards shall be based on the volume of cards requested and issued, and whether OSP determines that a bureau may more readily provide this service within its organization.

IRS-CI and FinCEN may delegate the issuance of courier cards/letters to subordinate administrative elements provided in all instances that advanced verification is made of each potential courier's security clearance status (level thereof), demonstrated and recurring need for a courier card and having received appropriate training. Records shall be maintained to account for names of recipients and corresponding courier card numbers and issuing offices are responsible for maintaining a supply of courier cards for their use. Additionally, pre-exit procedures shall be established to ensure courier cards are turned in by departing employees and contractor personnel and that accountability records are annotated accordingly.

All courier cards for SCI must be approved by the SSO on Treasury Department Form (TD F) 15-05.12, Request and Receipt for Courier Card; see Attachment 1. Requests for SCI cards must also include a justification explaining the individual's demonstrated and recurring need for issuance.

4. Basis for Issuing Courier Cards and Courier Letters

Courier cards shall be issued only to DO/bureau employees or cleared contractor personnel upon the demonstrated and recurring need and request of their DO/bureau organization. DO/bureau personnel security officials shall furnish clearance certification to the Director, OSP on potential recipients who engage in demonstrated and recurring courier activities to physically transport and securely deliver classified information. The person's electronically digitized color photograph (on a plain background) shall be provided to OSP in addition to their signature and printed name on a unlined index card. Since the signature is now scanned in, ensure the printed name and signature do not touch each other. Once digitized the signature card is destroyed.

Individuals attending an occasional meeting where classified information may be provided to participants no longer require a courier card. They do, however, have responsibility for maintaining classified information under their personal control and for returning the information to secure storage in the workplace. Attachment 1 is a sample courier letter format. Modifications include indicating the highest level of classified information and that SCI is authorized, when appropriate. It should also reflect the type

of identification the courier carries while serving in this capacity, e.g., Treasury/bureau credential number or employee PIV badge number, etc., and include pertinent identity verifying information.

Employees and contractor personnel transporting SCI or Top Secret information are required to coordinate in advance with the SSO and/or their Top Secret Control Officer. Hand-carrying SCI material is limited to the geographical limits of the Washington, DC Metropolitan area. The SSO may authorize hand-carrying of SCI material outside the Washington, DC Metropolitan area when specifically approved in writing by the Assistant Secretary, Office of Intelligence and Analysis or that official's designee.

5. Responsibilities and Training

a. *Courier Responsibilities.* Couriers are responsible for safeguarding classified information in their physical custody at all times while serving in that capacity. Non-official stops when transporting classified information are not permitted; pickup/deliveries shall be made from point-to-point unless more than one location is involved. Otherwise the courier goes directly to his/her destination or returns directly back to his/her office to bring the classified information under proper control and accountability within their organization. For SCI information the courier must bring classified information directly to the SSO. The SSO will then decide if that office will store non/SCI information or transfer custody, as appropriate.

b. *Safeguarding.* Under no circumstance shall the courier's person, pouch, briefcase, attaché, valise, package, or other container designated by the courier as being under his/her protection be opened, searched, viewed/read, or seized. Instances involving attempted or actual compromise of classified information during the courier process shall be reported to the DO/bureau security officer as soon as possible and made a matter of record with a copy of such report provided to the Director, OSP.

c. *Final Security Clearance.* Only individual employees and contractors with a **final security clearance** will be issued a courier card as warranted; those with an interim security clearance may only be issued a courier letter. All couriers shall be made familiar with the requirements in this section prior to issuance of a courier card/letter and designation of such individuals to serve as a courier and participate in required training. Such training will reinforce the requirement that their level of security clearance must be equal to (or may exceed) the level of

classified information they transport. Couriers shall surrender their courier cards to the issuing office upon request, termination of employment, or when the need for the employee or contractor to render demonstrated and recurring courier services is no longer valid.

d. *Training Requirement.* Issuance of courier cards may occur only after the individual has received training on his/her courier responsibilities as required by the Director, OSP. Couriers shall sign a receipt as evidence of their understanding of the requirements, practices and procedures at the time they are issued the courier card. Training shall be documented in the issuing office indices for tracking the life-cycle of security education and awareness during the courier's gainful employment. Training for couriers authorized to hand-carry SCI or another agencies SAP material shall be provided and documented by the SSO. All training shall include requirements for:

- Arranging for any overnight storage at an accredited U.S. Government or contractor facility and obtaining a receipt for temporary storage.
- Making a list of classified materials carried and leaving a copy thereof in the courier's office.
- Double wrapping materials and using an SSO-approved security pouch for SCI material.
- Arranging to have classified information shipped back via normal secure means, as warranted.
- Keeping classified material in their possession at all times.
- Reporting security incidents immediately upon arrival at an accredited U.S. Government or contractor facility or destination (whichever happens first).
- Not reading, displaying or using classified information in public.
- Never leaving classified material unattended.
- Never taking classified information home either before or after a meeting.
- Never storing classified information in a non-approved space or room.

- Following geographical travel limits of their authorization to hand-carry classified information, as applicable.

6. Treasury Department Form 15-05. 12, *Request and Receipt for Courier Card*

TD F 15-05.12, *Request and Receipt for Courier Card,* is the vehicle for initiating a request for a new courier card as well as a replacement for a lost/stolen and/or expired courier card. The form shall be signed by the employee's Director-level supervisor, provided to the organizations personnel security component for clearance verification and forwarding to the Director, OSP. TD F 15-05.12 is available at http://thegreen.treas.gov/policies/Forms1/Request%20and%20Receipt%20for%20Courier%20Card.pdf.

7. Treasury Department Form 15-05.7, *Courier Card*

The new (credit card sized) TD F 15-05.7, *Courier Card,* is the authorized courier card for use within the Departmental Offices for transporting collateral classified information (Top Secret, Secret, or Confidential) and SCI material for all courier cards issued after March 31, 2014. IRS-CI and FinCEN may continue to use the previous sized courier card for collateral cards. Courier cards shall be carried on the individual bearer's person when engaging in courier activity. Courier cards for collateral classified information and for SCI material shall have an expiration date of December 31st that is a maximum of five years from the date of issuance.

The front of each TD F 15-05.7 includes the bearer's photograph, legal name, partial social security number, signature, employing Treasury/bureau component, issue and expiration dates, and card number. To assist in safeguarding individuals' personal identifying information, courier cards show only the last 4 digits of the bearer's social security number, (e.g., XXX-XX-1234).

Contractors designated as demonstrated and recurring couriers shall be identified by the employing Treasury bureau for example as follows: DO-contractor, IRS- contractor, Mint-contractor, etc. The back of each card TD F 15-05.7 indicates the bearer is an authorized Treasury/bureau courier for classified information up to a specified level, for example, Top Secret, Secret, or Confidential or SCI material, as appropriate. In the event of injury, emergency, or death involving the courier, OSP is identified as the point-of-contact (POC), OSP is also the designated recipient in the event the courier card is lost or

stolen and to provide any potential finder with the appropriate address for returning the courier card to Treasury.

Attachment

1

Print Form Clear Form Data

Department of the Treasury
Request and Receipt for Courier Card

To be completed by requesting Supervisor

Employee Name _____ Date of Birth _____ SSN _____

Phone Number _____ Frequency of Courier Responsibilities _____

Treasury Bureau _____ Treasury Contractor _____

Requested Courier Level: Confidential [ ] Secret [ ] Top Secret [ ] SCI [ ]
(Check only one)

Supervisor's signature _____ Date _____

To be completed by Special Security Officer (for SCI only)

Special Security Officer's signature _____ Date _____

To be completed by Security/Issuing Office

Employee Reviewed Courier Training Module: Yes [ ] No [ ]

Clearance Verified: Yes [ ] No [ ]

Assigned Courier Card Number _____ Expiration Date _____

To be completed by Courier

Receipt is hereby acknowledged for the above courier card. I understand the courier card must be turned in to the security/issuing office when my services as a courier are no longer required.

Courier's Signature _____ Date _____

Notice The information requested is protected by the Privacy Act, 5 U.S.C. 552a which requires that Federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that the authority for soliciting your Social Security Number (SSN) is Executive Order 9397 which authorizes agencies to solicit SSNs for use as identifiers for administrative purposes. This form will be used as a means to prepare and issue a credential. Providing the information requested, including the SSN, is voluntary, however, if some or any part of the requested information is not provided, the effect will be that you will not be issued a courier card or be authorized to hand-carry and deliver classified information.

TDF 15-05.12

Attachment 2

[Treasury/Bureau Letterhead]

MM/DD/YYYY

SAMPLE COURIER LETTER FORMAT

This letter authorizes (NAME OF COURIER AND EMPLOYING DO/BUREAU ORGANIZATION) to serve as an official Department of the Treasury courier in accordance with requirements of Executive Order 13526 and the Treasury Security Manual, TD P 15-71.

Mr./Ms./Mrs. (LAST NAME) is assigned responsibility for physical protection and secure delivery of national security information classified (SPECIFY LEVEL, i.e., Top Secret, Secret or Confidential or SCI/SAP). This letter is valid for the conduct of official Treasury business for the period beginning (DATE MM/DD/YY)) and ending (DATE MM/DD/YY). Mr./Ms./Mrs. (LAST NAME) has been advised of his or her responsibilities in safeguarding classified information entrusted to him/her at all times while serving in this official capacity.

It is requested that Mr./Ms./Mrs. (LAST NAME) be afforded any special assistance, as may be necessary, to expedite his or her courier and related responsibilities. Verification of his or her status as an official Treasury courier can be obtained during routine business hours by calling telephone number (202) XXX-XXXX and after business hours on (202) XXX-XXXX.

Sincerely,

Name and Title of Issuing Authority

(SCI or another agencies SAP requires SSO signature)

Chapter V Section 7

Visitor Escort Requirements in Departmental Offices/Bureau Facilities

Updated 6/17/11

1. Introduction

This section identifies procedures when escorts are required to escort and assist visitors within Departmental Offices (DO)/bureau facilities. Use of escorts may be necessitated for an entire facility, work areas off limits to the public or certain areas restricted to designated and/or specially badged employees. Examples include, but are not necessarily limited to Sensitive Compartmented Information Facilities (SCIFs), secure rooms, approved open-storage areas, production areas, equipment/power vaults and generator areas, phone/wire closets, computer rooms and servers, restricted access work areas and the like.

2. Escort Time Frame

When escorts are required, visitors shall be accompanied by employees or authorized contractor personnel. Escorts shall accompany visitors at all times from their point of entry through point of departure. If visitors require a restroom break, the escort shall wait outside and resume escort duty when the visitor exits. Similarly, if short breaks are taken to obtain snacks, water, and the like, the escort shall remain with the visitor. Each escort is responsible for the visitor(s) he or she is assisting for the duration of the visit.

3. Visitor Screening

Every facility is unique and limitations on access are based on the nature of work being performed; classification or sensitivity of information; use or production of high-value or negotiable monetary instruments, equipment and/or manufactured items warranting specialized handling, accessibility, maintenance, monitoring or protection. Restrictions may further apply to those personnel who do not have access to particular information – whether it is classified, sensitive, pre-contract or procurement-sensitive.

VIPs visiting DO/bureau locations may warrant an escort to expedite their visit with senior officials. Extending such courtesy may consist of pre-screening in coordination with on-site security or uniformed officers and visit-sponsoring officials. Waivers may be granted to authorize use of external private entrances but only in coordination with and approval of on-site security or uniformed officials.

Visitors shall normally be directed to a central control point either in or immediately adjacent to the building lobby. In addition to being escorted, visitors are expected to

comply with established access control procedures which may include issuance of visitor/escort-required badges. After check-in, the visitor shall either call the sponsoring office hosting the visit (and/or for whom an appointment has been made), or be directed to a designated waiting area.

The office or individual sponsoring the visit is responsible for providing an authorized escort for the visitor(s). Escorts shall be one or more assigned employee or authorized contractor personnel responsible for accompanying visitors throughout the visit. The number of escorts may depend on the size of the group of visitors, for example, at least one escort per every 5 visitors is required for large groups. Such persons must be employed within and/or have authorized access to the particular area(s) being visited.

Visitors shall follow the escort's instructions and comply with internal sign-in procedures in particular areas being visited. This may include, but is not necessarily limited to relinquishing prohibited items such as personal digital assistants or blackberry communication devices, cellular phones, two-way pagers, photographic and recording equipment, etc. Internal work areas may also be equipped with visual displays such as colored lights or other readily discernable features in hallway and work areas to alert other occupant employees and authorized contractor personnel to the presence of uncleared individuals. All hallway and office doors not related to the visit shall be closed. See Chapter V, Section 1 regarding prohibited items, photography restrictions, and inspection of personal effects (paragraphs 13 through 15) for more information.

4. Escort Responsibilities

Escorts shall ensure that visitors are not inadvertently or unwittingly exposed to classified, sensitive or other items or material which they should not see, overhear, or otherwise obtain. This may require escorts to steer visitors away from desks, table tops, files, bookshelves, bulletin boards, etc. Visitors are NOT authorized to use Government-owned/operated computer or related IT systems. Any such attempt must be immediately reported to security officials. Escorts shall coordinate with and advise employees working in areas being visited that outsiders are in the vicinity and to exercise appropriate precautions. Simple rules include the following:

- If you observe anyone who is not wearing a badge, ask them if you can help.
- Politely inquire if they have a visitor's badge and if they do not, ask them to accompany you to the security or receptionist area.
- Do NOT try to restrain a visitor if they begin to walk away or resist efforts to help.

- Make a mental note of the visitor's description, what they are wearing, and immediately contact security, uniformed officers or administrative services personnel.

- Should there be any type of incident involving visitors, contact security or uniformed officials immediately.

5. Reporting Unusual Activities and/or Incidents

Any unusual activity involving visitors must be immediately reported to appropriate security officials immediately. Examples include but are not limited to attempts to use, read or download information from U.S. Government-owned/operated computer or related IT systems, introduction of USB "thumb" or "flash" drives, wandering away from escorts, walking into unlocked offices or rooms, attempts to use unauthorized electronic equipment, take photographs, etc. Reports shall include information as to who, what, when, where, how, with respect to the particular activity or incident.

Chapter V Section 8

Physical Security Requirements for the Treasury Secure Data Network

Dated 5/09/12

1. Introduction

This section identifies minimum physical security requirements for Treasury Secure Data Network (TSDN) networked (including docking station-equipped) computers installed in the Main Treasury and Annex Buildings. Additional security requirements for TSDN may be required in Departmental Offices (DO) satellite locations depending on the nature of each building, i.e., government-owned/occupied, commercial and/or multi-tenant office space where perimeter security features commence either at the buildings front entrance and/or the hallway/corridor office door from a publicly accessible elevator lobby. More stringent requirements may be applied beyond the minimum requirements identified herein by individual DO/bureau components to suit particularly unique needs and/or workspace configurations such as optional log registers in designated space(s) and use of external lock-boxes for personal electronics, etc.

The prescribed physical security requirements in this section are patterned after, but do not fully replicate, those required for safeguarding classified information in a Sensitive Compartmented Information Facility (SCIF). TSDN computers installed in an existing SCIF do NOT require additional safeguards beyond those required for certification and accreditation of the SCIF. TSDN computers planned for installation, incident to reconfiguration or construction of a new SCIF will be protected based on the SCIF features to be installed. In addition, and to the extent feasible, the requirements in this section are guided by Department of Defense national regulations and affiliated systems, i.e., SIPRNET-connected systems. Physical security criteria are governed by whether the work area is approved for closed storage, open storage, or continuous operations or a secure working area. Any open storage of classified information outside of a SCIF may ONLY be approved by the Director, Office of Security Programs (OSP).

TSDN work areas may be a room or group of rooms (suite) where TSDN terminals are installed for electronically processing Secret, Confidential, and/or sensitive information. TSDN work areas shall be afforded personnel access controls to preclude entry by unauthorized personnel. Non-Secret indoctrinated personnel entering a work area equipped with TSDN must be escorted by an indoctrinated employee/contractor who is familiar with established security procedures of that work area including the established means to alert assigned occupants to the presence of un-cleared persons and ensure classified discussions are curtailed, as appropriate. The physical security protections are intended to prevent and/or detect visual, acoustical, technical, and physical access by unauthorized persons. Identification checks, perimeter fences, police-type patrols and other security measures may be sufficient to be used in lieu of certain physical security or construction requirements.

2. Main Treasury and Annex Buildings

The Main Treasury and Annex Buildings comprise the Main Treasury Complex and have been designated by the Director, OSP as Level V in accordance with the Interagency Security Committee Standard, Facility Security Level Determinations for Federal Facilities, dated February 21, 2008. The Complex is immediately adjacent to the "18 acres" that comprise the White House, with on-site, 24/7 United States Secret Service (USSS) protection including the latter's external patrols of the perimeter. The resulting security-in-depth provides sufficient safeguards for collateral classified information; supplemental security controls are not necessary. The Main Treasury and Annex Buildings are also listed on the National Register of Historic Places raising special considerations with respect to deployment of particular security features.

a. Assigned Employees and Contractor Personnel – Permanent and temporary employees/contractors (including detailees, consultants and interns) working in DO offices equipped with TSDN must be United States citizens and hold at least an interim Secret security clearance. Un-cleared persons must be escorted at all times when visiting TSDN-equipped work areas and may never be left by themselves for any reason. Access to TSDN by foreign nationals on a U.S. Government or U.S. Government-managed equipment is not authorized. Repair/maintenance and administrative IT personnel with appropriate security clearance are exempt from unescorted access restrictions. Un-cleared persons are NOT authorized to access TSDN computer equipment installed in DO office spaces. Assigned office occupants shall NOT authorize the removal or alter the installed positioning of TSDN computer equipment.

b. Walls – Perimeter walls, windows, floors and ceilings will be permanently constructed and attached to each other. Any construction must be done in such a manner as to provide visual evidence of unauthorized penetration to include, where applicable, above false ceilings and below raised floors. No special construction is required for sound attenuation to preclude inadvertent disclosure of conversations; common sense should prevail during classified and/or sensitive discussions.

c. Hallway/corridor Doors – Hallway/corridor doors are those leading into/out of Main Treasury and Annex offices/suites which are accessible by all persons permitted unescorted access by the USSS to either building. Hallway/corridor doors are approximately 4' by 8' and either mahogany with single or 6-pane frosted glass, or wood paneled, and/or metal clad. Annex hallway/corridor doors are approximately 3'2" by 8' wood with a single frosted glass pane and/or metal clad. Every hallway/corridor door opening into space where TSDN is accessible shall be equipped with a deadbolt lock and keyed alike by security officials based on common organizations, e.g., International Affairs, Economic Policy, etc.

Doors must be plumbed in the frames and the frame firmly affixed to the surrounding wall. Where hinge pins are located on the exterior of the door, opening into uncontrolled areas outside the office space, the hinges shall be treated to prevent removal of the door. Door frames must be of sufficient strength to preclude distortion that could cause improper alignment of any door alarm sensors, improper door closure or degradation of any audio security. If a door must be kept open for any length of time (due to an emergency or other reason(s) it must be observable and controlled by a Secret-cleared person to prevent unauthorized access to, use of, and/or removal of TSDN. Office/suite occupants shall lock the hallway/corridor door and/or internal office doors (where TSDN equipment is located) when the space is not occupied by cleared persons. Locking the hallway/corridor also applies to the office space being temporarily empty while the assigned occupant(s) are at lunch or out sick or on extended leave.

d. Internal Office Doors – Internal office doors (within space first accessible via a hallway/corridor door) opening into work areas where TSDN is installed may have, but do not require, deadbolt locks such as spaces configured with only suite of individualized cubicle-type work stations. Office occupants are responsible for NOT leaving TSDN unattended and ensuring computers are logged off, disconnect and/or removed if NOT being used. Physical removal of TSDN work stations may be required when individuals are on detail or extended leave. Un-cleared personnel may NOT be assigned to work in (unused) internal office spaces where that are active TSDN computers no matter how temporary the assignment.

e. Windows – All windows which might reasonably afford visual observation of personnel, documents, material, or activities within the space, shall be made opaque or equipped with blinds, drapes or other coverings to preclude observation.

f. Alarms – Alarms are NOT required for areas with TSDN (outside a SCIF) in the Main Treasury and Annex Buildings.

g. Response Force – The USSS, Uniformed Division provides 24/7, on-site, and perimeter security for the Main Treasury and Annex Buildings. The Service also determines accessibility to these buildings based on their responsibilities for safeguarding the overall White House Complex (which encompasses the Main Treasury and Annex).

3. DO Satellite Offices

a. Assigned Employees and Contractor Personnel – The requirements for individuals working in the Main Treasury Complex also apply to all DO satellite offices. TSDN equipped space and systems shall only be used for appropriate government

work. The last person is exit is responsible for securing the space which includes putting TSDN laptops and encryption key away in the safe for most DO satellite offices.

b. Walls – Perimeter walls, windows, floors, and ceilings will be permanently constructed and attached to each other; including where anchored to or embedded into the floor or ceiling with supporting members and reinforced to true slab or the most solid surfaces. Any construction must be done in such a manner as to provide visual evidence of unauthorized penetration to include, where applicable, above false ceilings and below raised floors. Common sense applies to precluding inadvertent disclosure of conversations held within office spaces.

c. Hallway/corridor Doors – Hallway/corridor doors are those leading into/our of DO satellite offices/suites in commercial buildings which are accessible to the public. Hallway/corridor doors shall preferably be solid-wood or single glass pane equipped or metal glazing over wood, or constructed of composite material in steel frames. If featuring glazed glass at entrances the doors shall be constructed to facilitate orientation and safe movement in high-traffic areas. When metal cladding doors are used they shall be continuous and cover the entire front and back surfaces of the door with a minimum of 1 ¾ inch thickness. Perimeter doors must be plumbed in their frames and the frame firmly affixed to the surrounding wall. Door frames must be of sufficient strength to preclude distortion that could cause improper alignment of any door alarm sensors or improper closure. If doors are equipped with hinge pins located on the exterior side of the door where it opens into an uncontrolled area outside the office space, the hinges will be treated to prevent removal of the door (e.g., welded, set-screws, etc.).

d. Internal Office Doors – Interior doors (within space first accessible through a hallway/corridor door) opening into work space where TSDN is installed shall be flush, solid-core or of composite material construction. Frosted glass (single or multiple pane doors) that prevent clear viewing of the internal space may also be used within commercial suites.

e. Windows – Windows at ground level shall be constructed from or covered with materials which will provide protection from forced entry. The protection provided to windows will be no stronger than that of the contiguous walls. This requirement may be eliminated where the windows are alarmed, or made inoperable by either permanently sealing them or equipping them on the inside with a locking mechanism.

f. Alarms – Alarms are required in DO satellite office space only for ground level/first floor offices (with external facing windows) affording visual surveillance of personnel, document, materials, or activities within the facility. Subfloors and false ceilings do not require alarms. The maintenance program for intrusion detection, if any, shall ensure incidents of false/nuisance alarms are kept

to a minimum. If there is a problem with alarms, notify the Secure Service Desk (202) 927-1111 immediately.

g. Response Force – When alarms are installed, the response comes from the Federal Protective Service (FPS) and/or General Services Administration (GSA) contract guards; the USSS does NOT respond to alarms in DO satellite offices.

4. Bureau Locations with TSDN

Bureau locations with TSDN equipment shall have at least equivalent if not greater protection as in DO satellite offices with respect to wall, hallway/corridor door, internal office doors, windows, alarms and FPS/GSA response force or on-site internal security personnel, as applicable.

5. TSDN Security Education, Training and Awareness

Security education, training and awareness shall be provided to all individuals approved for access to TSDN commensurate with their respective responsibilities when using, operating, administering, and maintaining the TSDN including security-related procedures and risks. This includes application of required classified/sensitive markings, storage of classified information in GSA-approved security containers when not in use, and prompt retrieval of hard-copy printouts when produced on a shared printer. Physical security protections apply to all printed classified/sensitive information and especially extra or flawed copies. Do NOT abandon or throw intact into trash receptacles where they might be retrievable. Immediately shred any unwanted printed documents and if using "burn-bags" ensure the material is secured if classified and controlled if sensitive pending collection for destruction. Accounts for users who do NOT have a current training certificate or have not logged onto TSDN within the last 30 days are subject to being disabled.

6. Unauthorized Use of TSDN

For purposes of this section, unauthorized use includes: use, loading, or importing of unauthorized software, e.g. applications, games, peer-to-peer software, movies, films, music videos or files, etc., accessing pornography; unofficial advertising, selling, or soliciting (e.g., gambling, auctions, pools, stock trading, etc.), improperly handling classified information; gaining unauthorized access to other systems and/or networks; endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity; posting information to external news groups, bulletin boards or other public forums without authorization; or other uses incompatible with public service.

Once installed, TSDN computers must NOT be moved without prior notification to and approval of IT security officials in the Office of the Chief Information Officer (OCIO). Employees and non-IT contractors are NOT permitted to introduce or use unauthorized software, firmware, or hardware on TSDN or relocate or change out TSDN equipment or the network connectivity of equipment without proper authorization, attach any device(s) or modify any aspect of DO access control system(s), including card readers, motion detectors, or alarms. Do satellite office occupants are prohibited from security the services of any security contractor to alter the access control system(s), or install or alter any security device used for protection of classified information (including locks providing access to TSDN terminals) without written authorization from the Director, OSP.

7. TSDN Self-Inspection Reviews

Classified (and sensitive information) shall be safeguarded at all times. Safeguards shall be applied against loss, espionage, fraud, misappropriation or deniability of service. Such information shall be accessed only by authorized persons, used only for its intended purpose, retaining its content integrity, marked properly as required and appropriately destroyed when no longer needed. When not in active use all classified information must be stored in a GSA approved security container; open storage of classified information is not authorized in DO satellite offices. DO satellite offices shall have an approved means of destroying classified information either on-site or secure means of delivery to Main Treasury for destruction.

To ensure safeguards are in effect, periodic reviews of the adequacy of the safeguards for operational, accredited TSDN-installed equipment shall be conducted. To the extent possible, reviews are to be conducted by persons who are independent of the user organization and of the IT operation or facility. Any changes to the TSDN equipment or associated environment that affect the accredited safeguards or result in changes to the prescribed security requirements shall require reaccreditation. There shall also be in place safeguards to ensure each person having access to TSDN may be held accountable for his or her actions on the system. The attendant audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.

8. TSDN Access Control and Use

TSDN terminals shall not be left unattended no matter how short a period of time and must be logged-off when not in use. Corridor hallway doors in the Main Treasury Complex must be locked when the space is unoccupied; same applies to internal or external doors to TSDN work areas in DO satellite office space. If a door must be left open for any length of time due to an emergency or other reason(s), it must be controlled

(or under observation by a cleared employee/contractor) in order to prevent unauthorized access.

TSDN computers shall be disconnected and/or physically removed if not being used and/or doors to empty offices locked, in spaces temporarily empty while an employee is on detail or leave for an extensive period or new hire is being recruited. Un-cleared persons may NOT occupy TSDN-equipped work spaces during such periods. Those persons who no longer have recurring business into TSDN space shall (where applicable) shall have their unescorted access terminated and any access control systems in effect modified to delete them from the system. Where keypad devices are utilized for access control purposes they shall be installed in such matter that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers. Electronic control panels needed for access control shall be located inside the space. Exchange or sharing of badge-activated access cards is not authorized.

The following personally-owned electronic equipment may be introduced into TSDN equipped office space provided the space is not within a Sensitive Compartmented Information Facility: electronic calculators/spell-checkers, wrist watches and data diaries, receive only pagers and beepers, audio and video equipment with only a "playback" feature (no recording capability), or with the "record" feature disabled or removed, blackberry/cellular phones (with camera feature disabled) and radios. However, blackberry and cellular phone devices must be either turned off or (depending on the location practice) NOT permitted in TSDN space when classified discussions occur.

9. Supervisory Responsibilities

Supervisors shall ensure access to TSDN and to specified types of information (e.g., intelligence, financial data and/or proprietary to Treasury) under their purview is granted only on a need-to-know basis and all personnel having access are appropriately cleared. Additionally they shall ensure all users have the requisite security clearances and supervisory need-to-know authorization, and are aware of their security responsibilities before being granted access to the TSDN and promptly removing authorizations when access is no longer needed. Supervisory personnel shall advise OCIO security officials when access to TSDN is no longer required (e.g., completion of project, transfer, retirement, resignation) and observe policies and procedures governing the secure operation and authorized use of TSDN including use for official purposes only. Supervisors shall ensure employees immediately report incidents, compromise or suspected compromise, potential threats or vulnerabilities involving TSDN to appropriate security officials.

Chapter VI Section 1 | **Counterintelligence Program Overview** | Updated 6/27/11

1. Introduction

This chapter describes the Department of the Treasury, Office of Intelligence and Analysis (OIA), Counterintelligence (CI) Program. The CI Program includes policies and activities designed to detect, deter and/or neutralize Foreign Intelligence and Security Service (FISS) intelligence collection activities directed against Treasury's personnel, operations, information technology infrastructure, systems, and facilities. These activities may include CI awareness and related training; briefings and debriefings regarding foreign contacts, travel, and related information; CI preliminary inquiries; and CI/Cyber operations. All Treasury CI activities will be conducted within the framework of The National Intelligence Strategy, The National Counterintelligence Strategy, and Executive Order (EO) 12333 to "collect (overtly or through publicly available sources), analyze, produce, and disseminate…counterintelligence to support national and departmental missions."

2. Authorities

- National Security Act of 1947, as amended, 50 U.S.C. §§ 401 *et seq.*
- The Intelligence Authorization Act of 1995, 50 U.S.C. § 402 (2010)
- 31 U.S.C. § 311, *Office of Intelligence and Analysis*
- 31 U.S.C. § 313, *Terrorism and Financial Intelligence*
- *Department of the Treasury Intelligence Community Element Procedures for the Conduct of Intelligence Activities* (Draft)
- The Intelligence Reform and Terrorism Prevention Act of 2004, as amended
- Executive Order (EO) 12333, *United States Intelligence Activities*, as amended (2008)
- Presidential Decision Directive PDD/NSC-12 (5 August 1993)
- Presidential Decision Directive PDD/NSC-75 (28 December 2000)
- Intelligence Community Directive (ICD) 700, *Protection of National Intelligence (21 September 2007)*

3. Applicability

This chapter applies to all personnel employed by, assigned to, or detailed with the Department of the Treasury, and to all Treasury contractors and consultants (hereafter "Treasury personnel" or "Treasury employee").

4. Responsibilities

a. The Assistant Secretary for the Office of Intelligence and Analysis (Treasury's Intelligence Community Element Head) "shall implement aggressive security and counterintelligence initiatives to support the identification, apprehension, and, as appropriate, prosecution of those insiders who endanger national security interests," per Intelligence Community Directive 700, *Protection of National Intelligence.*

b. The Deputy Assistant Secretary (DAS) for Security shall establish and implement the CI Program in accordance with appropriate legal authorities and the provisions of this chapter, Treasury directives and policies, and Office of the Director of National Intelligence (ODNI) policies and procedures.

c. The Director, Office of Counterintelligence (OCI), shall manage and direct the Department's CI Program.

d. Departmental Offices and Bureau Heads shall support the implementation of an effective CI Program by ensuring that Treasury personnel are cognizant of, and in compliance with, Treasury CI Program policies and procedures.

e. Treasury personnel shall comply with Treasury CI Program policies and procedures and cooperate with authorized OCI activities. Failure to comply may result in administrative action, such as the withdrawal of approval for continued access to classified information.

5. Program Implementation

OCI may conduct the following activities:

a. CI Education and Awareness. OCI will develop and execute a CI Education and Awareness Program to ensure that Treasury personnel are aware of FISS intelligence collection activities directed against Treasury. Treasury personnel shall be made aware of their responsibility to report any effort to gain illegal or unauthorized access to classified or sensitive information, or if the employee is concerned that he/she may be the target of actual or attempted exploitation by FISS.

b. CI Collection, Analysis, Production and Dissemination. OCI may collect (overtly or through publicly available sources), analyze, produce and disseminate CI information, per EO 12333 and as codified in 31 U.S.C. § 313. CI collection activities may include debriefing Treasury personnel subsequent to foreign travel, or upon occasions that expose the employee to possible elicitation or collection activity. Based on the information collected, OCI may advise Treasury officials

regarding the threat, produce Intelligence Information Reports (IIRs), and/or open a CI preliminary inquiry.

c. CI Preliminary Inquiries. OCI may conduct CI preliminary inquiries into deliberate security compromises, security violations and computer intrusions with possible FISS involvement, reported or detected CI anomalies involving Treasury personnel or information systems, any indication of a potential insider threat or possible FISS contact with Treasury personnel, or any other matter of CI concern that requires further inquiry to resolve. Preliminary inquiries may result in an advisement to the Federal Bureau of Investigation (FBI), per Title VIII § 811(c) of the Intelligence Authorization Act of 1995 codified at 50 U.S.C. § 402.

d. CI Support to Other Agencies. OCI shall support requests for information and assistance in the conduct of CI investigative activities from other agencies' CI elements, when approved by the Director, OCI.

e. CI Cyber Activities. OCI will develop and conduct Information Technology (IT)-based CI activities in accordance with Director of National Intelligence directives and other applicable guidance. OCI will coordinate with Treasury's Office of the Chief Information Officer to ensure implementation of appropriate CI initiatives to protect national intelligence information and systems.

f. CI Support to Assure the Supply Chain and Protect Treasury Critical National Assets. OCI will provide CI support to assure the supply chain from foreign adversaries and provide CI support to Treasury's critical national assets.

g. CI Liaison with the U.S. Counterintelligence Community. OCI will conduct liaison with members of the U.S. CI Community and participate in working groups, information exchanges, and other fora.

Chapter VI
Section 2

Foreign Contact Reporting

Updated
7/11/11

1. Introduction

This section identifies the requirement and procedures for Treasury personnel to report foreign contacts, while ensuring personnel their privacy and freedom of association. This requirement seeks to ensure that security risks to Treasury personnel or to the U.S. Government are identified at the earliest possible opportunity and that protective steps are taken to avoid a compromise of U.S. personnel and national security interests.

The success of this program depends upon the security awareness of all Treasury personnel. Personnel should be alert to any suspected Foreign Intelligence and Security Service (FISS) activity. If an employee is unsure about the circumstances of a contact, the employee should consult with the Treasury Office of Counterintelligence (OCI).

2. Responsibilities

a. Presidential Decision Directive NSC-12 (PDD NSC-12) requires that Treasury personnel report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(2) The employee is concerned that he or she may be the target of actual or attempted exploitation by FISS.

b. Treasury personnel should also report contact with any foreign national who has attempted to establish recurring contact or seems to be actively seeking a close personal association, beyond professional or personal courtesies.

3. Procedures

a. The Office of Security Programs (OSP) will advise Departmental Offices (DO) personnel of the contact reporting requirement at the time they receive a security clearance for access to classified information.

b. Bureau security personnel will provide notification on the contact reporting requirements and process referenced in paragraph 3(a) to bureau employees. Reported contacts will be evaluated by bureau security officials and provided to OSP, and ultimately to OCI, for evaluation.

c. Treasury personnel are required to acknowledge having been briefed on the contact reporting requirements and procedures as provided on Treasury Department Form (TD F) 15-03.4, *Contact Reporting Requirement Acknowledgment*, attached to this section and available at http://intranet.treas.gov/security/forms/contact-reporting-form.pdf. Previous editions of the TD F 15-03.4 are obsolete. TD F 15-03.4 is generally used at the same time that employees are briefed regarding their access to classified information. The signed TD F 15-03.4 will be filed in the employee's personnel security folder and a copy may be provided to the employee upon his or her request.

d. When Treasury personnel make contact reports, the report will be evaluated and indications of PDD-NSC12 concern will be provided to OCI for appropriate action. OCI will analyze the reported information and may debrief the individual that submitted the report.

Attachment

Department of the Treasury
Contact Reporting Requirement Acknowledgment

Department of the Treasury and bureau employees are required to report all contacts with individuals of any nationality, either within or outside the scope of the employees' official activities, in which:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information and technology.

(2) The employee is concerned that he/she may be the target of actual or attempted exploitation by a foreign entity.

(3) The employee has contact with known or suspected foreign intelligence officers from any country.

The focus is on reporting questionable contacts by individuals of any nationality regardless of the status of relations between his or her foreign country (or third-country nationals) and the United States.

These reporting requirements are NOT intended to infringe upon the rights of Treasury/bureau employees' free association, but to reinforce their responsibility for safeguarding classified and sensitive information and technology.

By signing this form, the employee is acknowledging that he or she has been briefed on the Treasury Department contact reporting requirements and conditions warranting reporting. Contact reports may be submitted in person and/or in writing to their Treasury/bureau security office. That office shall evaluate the employee's report and notify Treasury's Office of Counterintelligence for appropriate counterintelligence information purposes.

Employee Name _____

Signature _____ Date _____

The completed form will be filed in the individual's Treasury/bureau security file and a copy thereof may be provided to the individual.

TD F 15-03.4 (7/11)

Chapter VI Section 3

Counterintelligence Awareness Training and Foreign Travel Program

Updated 6/27/11

1. Introduction

This section describes the Department of the Treasury Counterintelligence (CI) Awareness Training and Foreign Travel Program. It identifies security awareness training, CI pre-briefing and debriefing responsibilities, and requirements related to foreign travel. Receiving defensive security and CI briefings in advance of foreign travel helps to reduce the vulnerability of Treasury personnel and information to Foreign Intelligence and Security Service (FISS) collection efforts. Additionally, CI debriefings of Treasury personnel, following their participation in foreign travel, enable Treasury CI personnel to assess possible FISS targeting of Treasury personnel or information.

Office of the Director of National Intelligence, Intelligence Community Policy Memorandum 2007-700-3 requires that all personnel with access to Sensitive Compartmented Information (SCI) report all unofficial foreign travel and receive appropriate defensive security and CI travel briefings. Failure to do so may result in the withdrawal of approval for continued access to SCI, in accordance with Director of Central Intelligence Directive 1/20P.

2. Responsibilities

a. The Director, Office of Counterintelligence (OCI), will:

(1) Manage the Department of the Treasury's CI Awareness Training and Foreign Travel Program.

(2) Prepare and provide defensive security and CI briefings to Treasury personnel.

(3) Conduct CI debriefings as warranted to assess whether Treasury personnel or information were targets of FISS collection efforts.

b. Treasury personnel with security clearance will:

(1) Participate in defensive security and CI briefings and debriefings.

(2) Follow the conditions specified for Treasury Personnel with Access to SCI.

3. CI Awareness Training

CI Awareness Training is conducted to ensure that Treasury personnel are aware of the current FISS threat directed against the Treasury Department and the responsibility to report any suspected intelligence collection attempt to OCI. The CI Awareness Training Program includes the following:

a. Initial education and awareness briefings for Treasury new hires. Initial training includes, but is not limited to, an overview of the OCI mission, insider threat, technical threat, espionage indicators, FISS collection, elicitation and recruitment techniques, foreign contact and foreign travel reporting requirements, as well as how to protect against FISS threats.

b. Refresher briefings designed to reinforce and update awareness of CI threats, issues, and Treasury personnel responsibilities. OCI will provide annual CI refresher training to all Treasury employees.

c. Tailored CI briefings for specific Treasury personnel such as those traveling to foreign countries; hosting foreign visitors in Treasury facilities; visiting foreign diplomatic establishments; with access to SCI; with access to information assessed as being of high interest to FISS or terrorist organizations; engaged in activities that may put them at risk for FISS targeting; and others as appropriate.

d. Production and dissemination of CI awareness information to Treasury personnel via CI summaries, brochures, posters, and the OCI web site(s) on Treasury computer networks.

4. Foreign Travel Program

a. Treasury personnel with access to SCI:

(1) Unofficial Foreign Travel: In accordance with Office of the Director of National Intelligence (ODNI) policy, all SCI-indoctrinated Treasury personnel must report all unofficial foreign travel and receive appropriate defensive security and CI briefings. Treasury personnel shall use the *Unofficial Foreign Travel Reporting Form* (TD F 15-03.5) available electronically at http://intranet.treas.gov/security/forms/15-03.05.pdf on the Treasury DO Portal or from Treasury's Special Security Office (SSO) (also available as attachment 1 at the end of this section) to report all unofficial foreign travel at least 30 days prior to travel, if possible. This will allow OCI to schedule the necessary briefings. Emergency travel or other circumstance may preclude adherence to these reporting requirements. In these cases, reporting shall be accomplished as soon as possible. It is better to file a report late – even subsequent to foreign travel – than not at all. Failure to comply may result in the withdrawal of

approval for continued access to SCI, in accordance with Director of Central Intelligence Directive 1/20P.

(2) Official Foreign Travel. OCI is automatically informed via Treasury's official travel system when Treasury personnel travel on official Treasury business. OCI may contact the traveler to schedule a defensive security and CI briefing or may direct the traveler to an online defensive security and CI briefing.

b. Other Treasury personnel:

(1) Unofficial Foreign Travel: While not required, Treasury personnel *without* SCI access are encouraged to report unofficial foreign travel to OCI. Depending on the countries being visited, OCI may arrange a defensive security and CI briefing.

(2) Official Foreign Travel. OCI is automatically informed via Treasury's official travel system when Treasury personnel travel on official Treasury business. OCI may contact the traveler to schedule a defensive security and CI briefing or direct the traveler to an online defensive and CI security briefing.

c. Foreign Travel Debriefing Program. If, during foreign travel, a Treasury employee suspects that he/she may have been the target of FISS or is aware of anything else they believe might be of potential CI interest, SCI-indoctrinated Treasury personnel shall notify OCI upon return. The individual shall submit a completed Foreign Travel Debriefing Form to OCI and participate in a debriefing. Non-SCI indoctrinated Treasury personnel are also encouraged to report such incidents to OCI, complete a Foreign Travel Debriefing Form, and participate in a debriefing with OCI if requested. The Foreign Travel Debriefing Form is available electronically upon request from OCI and is attachment 1 at the end of this section.

Attachment 1

Department of the Treasury
UNOFFICIAL FOREIGN TRAVEL REPORTING FORM
ALL personnel with access to Sensitive Compartmented Information (SCI)

Office of the Director of National Intelligence, Intelligence Community Policy Memorandum 2007-700-3 requires that all personnel with access to SCI report all unofficial foreign travel and receive appropriate defensive security travel briefings. Failure to do so may result in the loss of access to SCI. Treasury personnel without access to SCI may also use this form to report unofficial foreign travel.

Please report all unofficial travel to the Special Security Office (SSO) at least 30 days prior to departure to allow time for scheduling defensive security travel briefings. While last-minute trips do arise, please notify the SSO as soon as possible to avoid the need to make exceptions to the 30 day prior notice.

Complete both sides of this form and email to "SSO" in the Global Address List. The information you provide on this form will be used to tailor the defensive security briefing to best match your foreign travel plans. You will be contacted prior to departure regarding the defensive security travel briefing. Any questions should be directed to the SSO at sso@do.treas.gov or sso@tsdn.treasury.sgov.gov

PART I -PERSONAL INFORMATION

Last 4 digits of SSN:_____ E-mail Address: _____
Last Name: _____ First Name: _____ MI: _____

PART II -ITINERARY OVERVIEW

Countries to be Visited	Major Cities	Date From	Date To

PART III -TRAVEL INFORMATION (check all that applies or attach itinerary)

1. Mode of Transportation

☐ Plane Carrier: _____
☐ Cruise Cruise Line: _____
☐ Train
☐ Rental Car
☐ Government owned Vehicle
☐ Privately owned Vehicle
☐ Other: _____

2. Reason for Travel

☐ Business
☐ Vacation
☐ Other:_____

Notice: The information requested is protected by the Privacy Act, 5 U.S.C. 552a. The authority for requesting this information is the National Security Act of 1947, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. 435(a) (3),(4). This information is necessary to evaluate your request for foreign travel and will not be used for any other purpose. Your Social Security Number will be used solely to record your foreign travel. Executive Order 9397 authorizes agencies to solicit SSNs for use as identifiers for administrative purposes. Providing the information requested, including the SSN, is voluntary; however, your failure to do so may result in the termination of SCI access.

TD F 15-03.5 (3/08)

Attachment 1 continued

PART III – TRAVEL INFORMATION (continued)

3. Are you traveling with a foreign national? ☐ Yes ☐ No If "Yes", list below:

Name of Foreign National	Nature of Association (Business, relative, friend, etc.)	Full Address	Citizenship

4. Are you planning to make contacts with foreign governments, companies, or citizens upon your arrival at this location? ☐ Yes ☐ No If "Yes", list below:

Foreign Government and/or Name of Company or Individual	Reason for Contact (Business, relative, friend, etc.)	Full Address	Citizenship

Additional Information:

Chapter VI **Counterintelligence Preliminary Inquiries** Updated
Section 4 6/27/11

1. Introduction

The Office of Counterintelligence (OCI) may conduct counterintelligence (CI) preliminary inquiries into deliberate security compromises, security violations and computer intrusions with possible Foreign Intelligence and Security Service (FISS) involvement, reported or detected CI anomalies involving Treasury personnel or information systems, any indication of a potential insider threat or possible FISS contact with Treasury personnel, or any other matter of CI concern that requires further inquiry to resolve. The nature of CI preliminary inquiries requires extreme discretion to protect national security and personal privacy interests. As such, sharing and access to this information shall be in accordance with applicable law, regulation and policy. OCI's preliminary inquiries shall determine whether the matter may be closed, resolved through the personnel security clearance process, or warrants referral to another office or agency.

2. General Authority and Principles

a. Within the parameters outlined in this Section, CI preliminary inquiries may be undertaken by authorized OCI personnel for the purpose of identifying potential threats to classified or sensitive Treasury Department programs, information, activities or personnel, in compliance with 50 U.S.C. § 402.

b. Only OCI personnel authorized by the Deputy Assistant Secretary (DAS) for Security to carry the Treasury CI badge and credential, per Section 6 of this chapter, may conduct Treasury CI preliminary inquiries.

c. Consistent with 50 U.S.C. § 402, the Federal Bureau of Investigation (FBI) shall be advised immediately of any threat, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.

3. Implementation

a. The DAS for Security and the Director, OCI, may authorize the conduct of an OCI preliminary inquiry.

b. Authorized OCI personnel (identified in 2.b. above) may conduct a CI preliminary inquiry into the potential threat, utilizing:

(1) Information that is publicly available;

(2) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics, or international terrorism investigation or activity;

(3) Relevant information arising out of a physical, personnel, or information security incident.

c. Requests for access to personnel security files shall be in writing and explain the justification for the access. Only those portions of the individual's personnel security file(s) that are relevant to OCI's preliminary inquiry may be considered. Such requests will result in a written report explaining the reason for such access and the result.

d. CI preliminary inquiries shall be confined to Treasury personnel, former personnel, detailees, and interns, and shall be a matter of written record.

e. A CI preliminary inquiry will result in one the following:

(1) The matter is resolved by OCI, and the case is closed.

(2) Administrative action is recommended by OCI or the DAS for Security.

(3) The matter is referred to OSP and resolved through the personnel security clearance process.

(4) The matter is referred for further investigation. Preliminary inquiries may result in an advisement to the FBI, per Title VIII § 811(c) of the Intelligence Authorization Act of 1995 codified at 50 U.S.C. § 402, when there are:

(a) Indications that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power;

(b) Indications that Treasury personnel may be engaged in intelligence activities on behalf of a foreign power; in international terrorism, or in other [foreign] hostile activities;

(c) Indications of unauthorized contact between a Treasury employee and persons who may be engaged in intelligence activities on behalf of a foreign power; in international terrorism; or in other [foreign] hostile activities; or

(d) Indications of FISS threats directed against Treasury personnel, programs, infrastructure, information technology systems, information, or activities.

(5) The matter is appropriately reported, and the case is closed pending additional information that might support further inquiries or other action.

4. Coordination

Upon request from the FBI, OCI shall coordinate access to Treasury employees, provide access to relevant information, and otherwise assist the FBI's investigation into referred matters.

5. Retention of CI Preliminary Inquiries

When there is no indication of foreign activity or contact, and a formal investigation is not opened, U.S. persons information shall not be retained by OCI and shall be disposed of appropriately.

Chapter VI
Section 5

Counterintelligence/Cyber

Updated
6/27/11

1. Introduction

The Office of Counterintelligence (OCI) will conduct Counterintelligence (CI)/Cyber activities, in concert with Treasury's Office of the Chief Information Officer (OCIO), to detect, deter, and/or neutralize Foreign Intelligence and Security Service (FISS) intelligence collection activities that target Treasury's information technology (IT) infrastructure. OCI will also undertake activities to detect and identify the unauthorized use and potential unauthorized disclosure of national intelligence on Treasury's classified IT infrastructure. Specifically, OCI is responsible for monitoring employees, contractors and service providers ("insiders") who have legitimate access to Treasury classified intelligence networks. These activities will be conducted in accordance with E.O. 12333, *United States Intelligence Activities*, Intelligence Community Directive (ICD) 700, *Protection of National Intelligence*, and Intelligence Community Standard (ICS) 700-2, *Use of Audit Data for Insider Threat Protection*, and other applicable national guidance, and direction.

2. Implementation

a. OCI will coordinate with OCIO to identify and deter FISS collection activities that target Treasury's IT infrastructure. This may include, but is not limited to, dissemination of threat information; advice and assistance activities; and activities designed to evaluate Treasury IT infrastructure.

b. OCI will coordinate CI/Cyber activities with the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and other non-Treasury entities, as appropriate.

c. OCI will establish an insider threat auditing capability to analyze and attribute user activity on classified intelligence networks, including intentional and inadvertent misuse or technical exploitation.

d. OCI will assist in the mitigation of potential damage to information on classified intelligence networks.

Chapter VI
Section 6

Counterintelligence Badge and Credential Program

Updated
11/2/11

1. Introduction

a. This section establishes policy for the procurement, issue, control, and disposition of the Department of the Treasury Counterintelligence (CI) badge and credential (hereafter referred to in the aggregate as "CI badge and credential"). It applies to all personnel authorized to use or possess these credentials.

b. All CI badges and credentials are issued under the authority of the Office of Intelligence and Analysis to conduct CI activities pursuant to Executive Order 12333, 31 United States Code (U.S.C.) § 311, and 31 U.S.C. § 313. The Deputy Assistant Secretary (DAS) for Security is the Approval Authority for all CI badges and credentials. As such, the DAS for Security exercises oversight authority over the CI Badge and Credential Program. The Director, Office of Security Programs, is the authenticating official.

2. Issuance and Use of the CI Badge and Credential

a. **Purpose:** The CI badge and credential identify the bearer as a duly accredited Counterintelligence Officer of the Department of the Treasury who is performing official CI duties. The CI badge and credential empower the bearer during an official mission to represent the Department of the Treasury on CI and national security matters, to conduct CI preliminary inquiries within the scope of assigned duties, and to make CI investigative advisements to the FBI pursuant to Section 811 of the Intelligence Authorization Act of 1995 [50 U.S.C. § 402].

b. **Issuing Authority:** The DAS for Security is designated the Approval Authority for CI badges and credentials.

c. **Issuance:** The CI badge and credential may be issued to personnel who:

(1) are at least 21 years old;

(2) possess a final Top Secret security clearance based on a Single Scope Background Investigation;

(3) are Department of the Treasury permanent civilian employees in job series 0132 assigned to the Treasury Office of Counterintelligence (OCI);

(4) and, who have successfully completed a recognized federal or DoD CI investigations course that resulted in issuance of a CI badge and credential. Such courses include, but are not limited to the Air Force Office of Special Investigations (AFOSI) basic investigations course, US Army basic CI agent's course, the Naval Criminal Investigative Service (NCIS) agent's course, and other federal basic CI investigations courses that culminate in the issuance of a badge and credential. The DAS for Security will determine those courses recognized as meeting this requirement.

d. **Use:** The CI badge and credential will only be used when needed to fulfill official responsibilities during the performance of assigned missions as a means to establish identity and affiliation, and obtain access and appropriate assistance required by the mission, such as in conducting a CI preliminary inquiry.

e. **Retention:** The CI badge and credential will be retained for the duration of assignment to OCI. The CI badge and credential must be immediately surrendered at the end of this assignment or at any time as directed by the DAS for Security.

3. Processing Requests for the CI Badge and Credential

Submit CI Badge and Credential Issue Request and Authorization form to the Director, OCI, for concurrence, prior to submitting to the DAS for Security for approval. Upon approval by the DAS for Security, the OCI badge and credential custodian will issue the CI badge and credential to the approved requestor. The recipient will sign an Acknowledgement of Receipt and Proper Use of CI Badge and Credential form at the time of issue.

4. Loss of CI Badge and Credential

a. Upon discovery of the loss of a CI badge, credential, or blank credential form, the accountable individual will notify the Director, OCI, and will conduct an immediate search of the suspected loss area. The Director, OCI, will take the following actions:

(1) Conduct an immediate recovery search.

(2) Notify the OCI badge and credential custodian and DAS for Security by the fastest means available.

(3) Appoint an officer to investigate the loss and report the results to the DAS for Security and OCI badge and credential custodian. The DAS for Security will notify local and national investigative agencies, as appropriate.

b. The DAS for Security may approve relief from accountability for the lost CI badge and credential only upon satisfactory review of the investigative results and any corrective actions.

c. Loss of a CI badge or credential may be sufficient basis for disciplinary action and removal from CI duties.

5. Misuse of the CI Badge and Credential

a. Individuals involved in the misuse of CI badges or credentials may be subject to criminal and civil penalties. Additionally, use of the CI badge or credential for other than official duties is sufficient basis for disciplinary action and removal from such duties. The following is representative of misuse of the CI badge and credential:

(1) Falsifying, forging, altering, or tampering with a badge or credential.

(2) Photographing or copying a badge or credential.

(3) Using a badge or credential to gain access to information, facilities, or persons not required/authorized in the performance of official duties.

(4) Using a badge or credential as identification when not on official duties.

(5) Using a badge or credential to perform functions not within the mission or authority of the element to which an individual is assigned or attached.

(6) Using a badge or credential to perform functions which may be prohibited under the provisions of Treasury directives.

(7) Using a badge or credential in an attempt to avoid civil citations, such as off-duty traffic or parking tickets.

b. Upon discovery of an alleged act of misuse, the Director, OCI, will:

(1) Immediately notify the DAS for Security of the nature and details of the allegation.

(2) Withdraw the badge or credential and return them to custodian control until the allegations are resolved.

(3) Coordinate with the DAS for Security to identify an appropriate inquiry officer to investigate the allegation.

(4) Forward the result of the inquiry to the DAS for Security in a formal report.

(5) Initiate administrative or disciplinary action, as appropriate, after consulting the DAS for Security, based upon the results of the inquiry.

6. CI Badge and Credential Controls

a. **Safeguarding Badges and Credentials:** CI badges and credentials, to include badge dies, credential masters, blank credential forms, and credentials of authorized personnel whose current duties do not require their use, will be maintained in an authorized repository under the control of a duly appointed Treasury CI badge and credential custodian.

b. **Badge and Credential Custodians:** The Director, OCI, will appoint primary and alternate badge and credential custodians in writing. Custodians are responsible for the accountability, control, processing, and safeguarding of badges and credentials within the OCI badge and credential repository.

c. **Storage and Disposition Requirements:**

(1) The CI badge and credential repository will be securely stored at all times in a GSA-approved security container. Custodians will maintain continuous accountability by badge number and credential control number for each badge and credential maintained.

(2) CI badge and credential custodians will immediately return to the repository all issued CI badges and credentials upon an individual's retirement, resignation, termination, or permanent reassignment to duties no longer requiring the CI badge and credential.

d. **Inventories:** All CI badges and credentials will be visually inspected for damage during inventories. Inventory records will be maintained as permanent records. CI badge and credential custodians will conduct 100 percent physical inventories of all CI badges and credentials issued or on-hand on the following occasions:

(1) Annually during the last quarter of each calendar year.

(2) Upon any change of primary custodian. Such inventory will consist of a joint inventory by the outgoing and newly-appointed custodian. The inventory will be conducted sufficiently in advance to allow verification and clarification of any discrepancies, but in no case will such inventory begin later than 10 duty days prior to the departure of the current custodian.

(3) When so directed by the Director, OCI, or the DAS for Security.

7. CI Badge and Credential Trophy Program

a. OCI personnel may obtain the CI badge and credential in trophy form upon retirement or separation from the Department of the Treasury, provided the individual:

(1) was authorized a CI badge and credential during their assignment;

(2) was not removed from Treasury CI duties for cause; and,

(3) served a minimum of five years in OCI.

b. Eligible individuals who wish to obtain a CI badge and credential trophy will do so at their own expense. The CI badge and credential trophy order will be processed by the CI badge and credential custodian and approved by the Director, OCI.

Chapter VII
Section 1

Security Access Controls for the Main Treasury Complex

Updated
4/22/14

1. Introduction

For security purposes, the Main Treasury Building at 1500 Pennsylvania Avenue, NW, Washington, DC and the Treasury Annex Building at Madison Place, NW, are considered part of the White House Complex. Collectively, the Main Treasury and the Treasury Annex are known as the Treasury Complex and both structures are owned and occupied by the Federal Government.

The United States Secret Service (USSS) establishes and executes security practices and procedures for access to the White House. USSS has jurisdictional control over security practices and procedures for access to the Treasury Complex and the adjoining grounds. The USSS coordinates with the Director, Office of Security Programs (OSP), to develop and refine security practices, procedures and requirements for employees, contractors and visitor access to the Treasury Complex.

This section promulgates security access controls for the Treasury Complex affecting Departmental Offices (DO)/bureau employees, detailees (persons on temporary assignment to DO from other Government agencies/departments), and other Federal employees; including law enforcement officials, consultants, visitors and contractor personnel. Except for activities performed by the USSS, which are limited to the Treasury Complex, practices and procedures herein may also be utilized by bureaus in controlling access to their facilities and office space.

2. Treasury Security Responsibilities

a. *Deputy Assistant Secretary (DAS) for Security.* The DAS for Security has the primary responsibility for advising senior Treasury officials with respect to security controls for access to the Treasury Complex.

b. *Director, Office of Security Programs (OSP).* The Director, OSP, has responsibility, in coordination with the USSS, for establishing practices and procedures to maintain adequate security for safeguarding personnel, property, equipment and information within the Treasury Complex including processing and issuance of access badges. DO employees, detailees, interns, consultants and contractors are required to cooperate with OSP security requirements regarding access badge procedures. OSP security officials work closely with USSS on issuance of DO access badges in accordance with Homeland Security Presidential

Directive 12 (HSPD-12) affecting activities that are authorized to occur internally, on the external premises of the Treasury Complex, and on related security matters. At the Director's discretion, that official may revoke an employee's badge access privileges to the Treasury Complex when an employee has been determined to have committed multiple security infractions involving their loss of a PIV access badge.

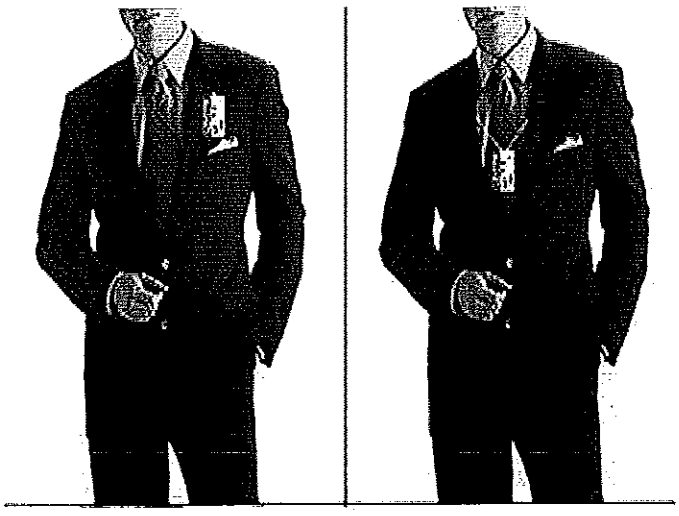
3. Designating Security Point-of-Contact

In accordance with Treasury Order 105-19, "Delegation of Original Classification Authority; Requirements for Downgrading and Declassification," DO offices reporting to an Assistant Secretary or a higher official must designate one or more Security Point of Contact (SPC) in writing to the Director, OSP, as a liaison with OSP officials. SPCs are responsible for coordinating with OSP for security services, e.g., issuance of keys, access badges, credentials, new/changing locks, opening locked hallway doors, reporting thefts/incidents, safe/alarm repairs, combination changes, inquiries about and using security forms, handling and marking classified and/or sensitive information, scheduling burn-bag pickups, disseminating security information, scheduling office employees for security training, etc.

4. DO Access Badges/ID Cards

a. *DO Access Badges and ID Cards.* DO access badges are U.S. Government property issued in accordance with Homeland Security Presidential Directive (HSPD) -12 under tight control and accountability. Further information on use of HSPD-12 access badges/ID cards is available at www.fedidcard.gov. Upon terminating DO employment, DO access badge-holders, contractors, consultants and detailees are required to surrender all DO-issued badges, credentials, courier card, keys, etc, to the OSP.

b. *Employee Access.* DO badges are valid for a maximum period of 5 years except for those on fewer year employment appointments. DO badge-holders must present their access badge to the USSS officer upon entering the Treasury Complex and use the badge reader (and 4 digit PIN number) feature to open the turnstile. Badge-holders select their own PIN number at the time the badge is issued; the PIN number is not required to exit. While inside, badge-holders must visibly wear the DO access badge on a



lanyard, chain, or clip on their person ***displayed above the waist*** as illustrated. Upon exiting the premises, badge-holders should remove and safeguard their access badge. At the time of renewal, employees are required to submit a new Work Order Access Pass Application form (TD F 15-05.1888) to the OSP for continued access to the Treasury Complex.

5. Visitor and Other Treasury Bureau/Other Government Agency Employee (OTB/OGA) Access

a. *Visitor Access.* Visitors with appointments are issued a temporary badge for access that must be visibly displayed on their person ***above the waist*** in the same manner as DO badge-holders at all times during their visit. Visitor access badges must be scanned using the badge reader feature for access. Visitors must surrender the temporary badge upon exiting the Treasury Complex. See Chapter V, Section 7, "Visitor Escort Requirements to DO/Bureau Facilities.

b. *Other Treasury Bureau/Other Government Agency employees* (OTB/OGA). OTB/OGA employees may be authorized unescorted access during regular business hours (7:00 am – 6:30 pm, Monday-Friday) for a period of six months. Access authorization terminates if OTB/OGA employees do not enter the Treasury Complex during a six month period. Access requests for OTB/OGA employees must be submitted by their respective Physical Security (or equivalent) Officer on a Treasury Pass Application form (TD F 15-05.1888) along with a statement of need addressed to the Director, OSP, validating the reason(s) for access to the Treasury Complex; this requirement is waived for Bureau Heads. The statement must include:

1. Purpose of Visit
2. Frequency of visit(s)
3. Visit location (office/room number)
4. Name of Treasury Point of Contact

Applicants will be notified by email when an appointment has been made for them to have their PIV access badge encoded for Treasury access. For this process individuals must know their 6 – 8 digit PIN that was established during their initial badge activation. Individuals who do NOT know their 6 – 8 digit PIN, must report to their respective security office to establish a new PIN before

coming to their appointment at Main Treasury. Note that access to Main Treasury terminates after a certificate rekey or badge reissuance action. Secret Service will update badges in their Physical Access Control Database without requiring appointments but will require a new TD F 15-05.1888 whenever the expiration date on a badge is changed (as in a badge reissuance).

c. *Detailed Employees.* Detailed employees may be authorized unescorted access during regular business hours (7:00 am – 6:30 pm, Monday-Friday) for the period of their detail. Detailees must submit the Treasury Pass Application to OSP for processing and wear their PIV badge visibly displayed on their person ***above the waist*** in the same manner illustrated for employees.

d. *DO Contractors.* Contractors may be authorized unescorted access during regular business hours (7:00 am – 6:30 pm, Monday-Friday) for a maximum period of 3 years. Contractors are not normally granted 24/7 access or escort privileges to Main Treasury unless required by the Statement of Work (SOW). DO Contractor PIV issuance is initiated by their Contracting Officer's Representative (COR) for contractors with a period of performance greater than 180 days. Contractors must be entered in to Human Resource Connect (HRC) and the COR must submit the Treasury Pass Application for PIV card issuance to OSP. The distinct contractor badge must be visibly displayed ***above the waist*** in the same manner as employees. All DO-issued HSPD-12 contractor badges shall be surrendered to security officials when the contract for which the access badge was issued is completed (or terminated) and/or on the contractor's departure.

(1) Contractors needing a background investigation must be entering into HRC by their COR. Required fingerprints are captured through the USAccess enrollment process. Note that the contractor's personal (home/campus/dorm) email address is required along with the COR's email address. Business addresses are reserved for DO employees and can be left blank.

(2) Contractors with a Period of Performance of 180 days or more must be entered by the COR in HRC. CORs shall also indicate whether access is required to one of the following:

(a) Other DO facilities, as appropriate, i.e., 1801 L Street, Metropolitan Square, 1750 Pennsylvania Avenue, etc. and/or Treasury Complex with no computing systems (LAN) need.

(b) Contractor access to DO computing systems (LAN) is required but no access to DO facilities.

(c) Contractor requires access to DO facilities and LAN.

(3) CORs shall no submit TD F 15-05.1888 until they have entered contractors into HRC. For contractors requiring access to the Treasury Complex, the COR must submit the original TD F 15-05.1888 to OSP bearing the contractor's signature and date of the application. Contractors who do NOT require access to the Treasury Complex shall have their COR submit a scanned TD F 15-05.1888 to OSP bearing the contractor's signature and application date.

6. HSPD-12 Background Check, Expired Badges and Access Denial

a. *Personal Identity Verification (PIV).* DO employees and contractors including those assigned to DO satellite office space undergo a background investigation under HSPD-12 to receive a photo-bearing DO access badge and PIN number to enter the Treasury Complex. HSPD-12 badges show the expiration date on the face of the badge. Visit the OSP website for more HSPD-12 information at http://thegreen.treas.gov/programs/Pages/publications.aspx. USSS uses an individual's state issued driver's license as the primary identifier for initiating a background check following the individual's submission of Main Treasury TD F 15-05.1888. The previous form (OF 71-11.6) may still be used until existing supplies are depleted.

b. *Expired Badges.* When a USSS officer determines that an access badge has expired, the officer will confiscate take the badge and notify the individual to contact the OSP for reissuance, renewal and/or resolution. To gain access if the badge has expired, the individual(s) will need to be entered into the Treasury Appointment Center (TAC) access system by the employing office.

c. *Access Denial.* If a USSS officer determines that there is cause for denying access to the Treasury Complex the person will be so notified. In some cases an individual may be placed on "Escort Only" and a DO employee must escort the individual at all times while in the Treasury Complex. Specific individuals placed on a "Do Not Admit" list by USSS will be barred from the Treasury Complex. Notification of the reason(s) for access denial or, escort only, or do not admit, shall be provided as appropriate. When USSS prevents an individual's access to the Treasury Complex the individual may appeal in writing to the Director, OSP,

and/or the USSS Inspector. Failure to complete Electronic Questionnaires for Investigations Processing (EQIP), the Questionnaire for National Security Positions (SF 86) and/or requested documentation can result in interruption of or limited access to Main Treasury Complex and DO satellite office buildings or designation as "Escort Required".

7. Forgotten/ Lost Badges and Reporting/Replacement

a. *Forgotten/Lost DO Access Badges.* Badge-holders who have forgotten their DO access badge must present the USSS officer at post with an alternate photo ID, e.g., driver's license, U.S. passport, DO ID, or other acceptable identification process, bearing the same name as that on their lost/missing DO access badge. Acceptable forms of ID include those listed on the Department of Homeland Security, U.S. Citizenship and Immigration Services, Form I-9, (last page) available at http://www.uscis.gov/sites/default/files/files/form/i-9.pdf. A temporary access badge may be issued by the USSS officer upon verification of the person's identity in the USSS' access control database as having been issued a DO access badge. The bearer's permanent access badge will be electronically deactivated pending the badge-holder's return with their forgotten or misplaced badge.

b. *Reporting Lost and Issuing Replacement Access Badges.* Employees, detailees, interns, consultants and contractors who have lost their access badge must report the loss in writing (e-mail will suffice) to OSP within 24 hours. Reports of lost badges shall include the date, place and circumstances surrounding the loss. In reissuance cases, the entire registration and issuance process (including fingerprint and facial image capture) is repeated. OSP will verify that the employee, detailee, intern, consultant or contractor remains in good standing and their personnel records are current before reissuing the badge and associated credentials. Processing of a new TD F 15-05.1888 through USSS is also required.

c. *Treasury USSS Database (OPOST Computer).* Information in the Treasury USSS' Database (OPOST Computer) may only be retrieved and accessed through a USSS Treasury/Annex entry post. USSS officers do not have access to the OPOST Computer at exterior areas and USSS posts surrounding the White House Complex. Accordingly, verification of DO badge-holders' identification may only be validated at an interior entry post.

8. Badge Restrictions

Badge Access Privilege Restrictions. Upon a determination by the Director, OSP that the repeated loss by an individual of two or more building access badges may pose a security risk, the Director may determine that such employee, detailee, consultant or contractor should not be issued a replacement badge for access to the Treasury Complex. In these circumstances, the individual may be placed on a work order requiring the issuance of a temporary badge for continued daily access to the Treasury Complex.

(1) Badge access restrictions may also be applied if an individual does not follow prescribed security instructions, procedures or manifests inappropriate conduct or behavior that may be disruptive, threatening or injurious to the safety and well-being of others (including the Treasury Complex). This includes questionable judgment, lack of candor, dishonesty or compliance that raises questions about an individual's reliability, trustworthiness and protection of classified and/or sensitive information. Of special interest is any failure to provide truthful and candid answers during the security process.

(2) Examples include, but are not necessarily limited to the repeated failure to complete the Electronic Questionnaires for Investigations Processing (e-QIP) and associated security release forms; not responding to verbal/written requests from security officials for further information, not attending required security training when requested in compliance with requirements for those holding a security clearance for access to classified information. When badge access restrictions are put into effect the individual will be so notified and may appeal to the Director, OSP for relief or reconsideration. The Director's decision is final.

9. Responsibility for Collecting Badges for Destruction

a. *Responsibilities of Administrative Contacts, Supervisors and Contracting Officer Representatives.* When an employee or contractor separates voluntarily or involuntarily from DO (retirement, transfer, resignation, change of position or work assignment, termination or end-of-contract) the administrative contact, supervisor or contracting officer's representative is responsible for collecting their access badge for destruction by OSP. In the case of an employee or contractor determined to be using a fraudulent identity or the individual is deceased, an attempt at badge retrieval shall be made, or report thereof, as appropriate.

b. *PIV Access Badge Destruction.* PIV access badge destruction must occur within 24 hours of an individual's departure from the Departmental Offices. In accordance with FIPS 201, a badge-holder shall apply for reissuance of a new PIV badge if the old PIV badge has been compromised, lost, stolen or damaged. In case of an emergency affecting the safety and security of the Treasury Complex, assigned personnel and/or visitors, information and systems, the PIV badge can be immediately deactivated and if possible the badge will be collected from the departing individual and destroyed. In reissuance cases, the entire registration and issuance process (including fingerprint and facial image capture), shall be repeated. OSP will verify that the employee or contractor remains in good standing and their personnel records are current before reissuing the badge and associated credentials. Processing of the Work Order Access or Pass Application through USSS is also required.

10. Treasury Complex Working Hours and Entrances/Exits

Regular business hours in the Treasury Complex extend from 7:00 AM to 6:30 PM, Monday through Friday and the schedule periodically updated by OSP and posted at http://thegreen.treas.gov/policies/Policies/Ch7_Sec6%20Schedule%20for%20Main%20Treasury%20Complex%20Entrances.pdf. Visitors may enter the Treasury Complex at two access control points; Pennsylvania Avenue (Main Treasury) and Madison Place across from Lafayette Square (Treasury Annex). Mobility impaired persons may use the entrances at Fifteenth Street NW for Main Treasury and the alleyway off Pennsylvania Avenue NW for the Treasury Annex.

11. Secretary of the Treasury's Private Entrance

The Secretary's private entrance is reserved for the current Secretary, the Deputy Secretary and their appointments as cleared in by the Secretary's office with the USSS. DO access badge-holders may only use the Secretary's private entrance when authorized and/or while accompanying the Secretary or Deputy Secretary and must display their badge to the USSS officer.

12. Non U.S. Citizen Visitors to the Treasury Complex

Visitors to the Treasury Complex who are neither U.S. citizens or in a lawful permanent resident status will be escorted at all times. Those individuals will be escorted by one or more DO access badge-holders that meet escort requirements. See Chapter V, Section 7, "Visitor Escort Requirements in DO/Bureau Facilities". Non-U.S. citizen DO employees

who have lawful permanent residency status (green card holder) are authorized unescorted access to the Complex while working for DO.

13. Visitor Appointments

a. *Visitor Appointments.* Appointments for visitors must be made electronically to the Treasury Appointment Center (TAC) via the DO LAN. The following procedure is required for access to the Treasury Complex:

(1) Appointment groups less than 50 people must be submitted to the TAC 24 hours in advance of the expected visit.

(2) Appointment groups of 50 or more people must be submitted to the TAC 72 hours in advance of the expected visit.

(3) Foreign national appointments must be submitted to the TAC 48 hours in advance of the expected visit.

b. *TAC Operating Business Hours.* Business hours for the TAC are from 6:00 AM to 6:00 PM, Monday through Friday. Between 6:01 PM and 5:59 AM (and on weekends and holidays), all visitors must be escorted by a DO access badge-holder. Only DO employees housed in the Treasury Complex may schedule appointments. The Treasury Appointment form is available at http://thegreen.treas.gov/policies/forms/Pages/TreasuryAppointment.aspx. All mandatory blocks on the electronically generated appointment form must be completed to be accepted by USSS.

c. *Scheduled Appointments.* Appointments are valid for one hour on either side of the time of the scheduled visit, e.g., a 9:00 AM appointment holder may arrive as early as 8:00 AM or as late as 10:00 AM. If the visitor arrives before or after this "window" the individual's name will not appear on the USSS officer's entry post computer and will have to be resubmitted to the TAC.

d. *Personal Information.* Employees, detailees, contractor personnel and visitors are required to disclose their social security number and date of birth (SSN/DOB) as a condition of being considered for access to the Treasury Complex. Disclosure of the SSN/DOB is used solely as identifying information due to the large number of people who have identical names and birth dates and whose identities may only be distinguishable via their SSN/DOB. This information is

required for individual appointments to be entered into the TAC. Providing the information is voluntary, however, failure to disclose the SSN/DOB may result in an individual's not being considered for access to the Treasury Complex. Solicitation of the SSN is permitted by Executive Order 9397. DO employees who obtain SSN/DOB information in order to make scheduled appointments for visitors are required to protect such personally identifiable information from unauthorized access, misuse or abuse.

e. *Delivery Appointments.* Appointments for delivery of supplies, equipment, furniture, foodstuffs, etc. via the Treasury Moat or Annex loading dock must be received by USSS before 2:00 PM the day before the delivery. Only DO employees working inside the Treasury Complex may submit the Treasury Moat Delivery Form at http://thegreen.treas.gov/services/mail/Pages/moatdelivery.aspx. All mandatory data blocks on the form must be completed before it can be accepted by the Office of Facilities and Support Services and the information relayed by that office to USSS.

f. *Pass and Lock Section.* The UD Pass and Lock Section is responsible for issuing permanent DO access badges, green intern "I" badges and office keys to DO employees at the direction of the OSP. In addition, the Pass and Lock Section fingerprints all new employees in accordance with HSPD-12. **Operating hours are from 7:00 AM to 12:00 PM and again from 1:00 PM to 2:30 PM, Monday through Friday. The Pass and Lock Section is reached via the hallway entrance to room 1015, Main Treasury (and inside to the right in room 1600).**

14. Visitor Escort Requirements

Visitors to the Main Treasury and Annex Buildings who are neither U.S. citizens or in a lawful permanent resident status will be escorted at all times by one or more Departmental Offices (DO) employee access badge-holders. Escorts are required for all visitors permitted access to work areas otherwise off limits to the public and certain areas restricted to designated and/or specially badged employees. Items such as personal digital assistants or blackberry communication devices, cellular phone, two-way pagers, photographic and recording equipment (per paragraph 14b) may not be used and/or must be locked in available storage bins for the duration of the visit. See Chapter V, Section 7 for additional information.

15. Tours of the Historic Main Treasury Building

Guided tours of the historic Treasury building are available by contacting the Curator's Office. The tour features restored office spaces such as the marble Cash Room (the adjoining Grant Room), the office of Salmon P. Chase, Secretary of the Treasury during the Civil War, and the temporary office used by President Andrew Johnson following Abraham Lincoln's assassination; the latter restored to its 1860s appearance. The formal tours include Congressional tours, VIP (Professional Courtesy) tours, Special Holiday/Summer (Treasury employees only) tours and those specifically requested by Assistant Secretary and higher level officials.

a. *Weekend Tours.* Weekend tours are scheduled in advance through Congressional offices. Tours are only available for U.S. citizens and legal permanent residents. The name, date of birth and social security number must be provided for each visitor and those 16 years and older must have photo identification with them on the date of their scheduled tour. There are 4 weekend tours on most Saturdays between March and December at 9:00, 9:45, 10:30 and 11:15 each morning. There are no tours on Federal holiday weekends or when special events/meetings are held to conduct official weekend business. Weekend tours are limited to a maximum of 12 persons with two docent or Treasury employee escorts.

b. *Weekday Tours.* The size of weekday tour groups is limited to 8 persons accompanied by their guide (docent or Treasury employee). For any tours exceeding that number the requesting Departmental Office shall provide additional employee escort. Weekday tours no longer include the Salmon P. Chase suite. Each visitor's name, date of birth, social security number and photo identification is required.

c. *VIP (Professional Courtesy) Tours.* These VIP tours are reserved for visiting academics, historians, other agency curators, and such benefactors as the Treasury Historical Association and conducted by the Curator's Office.

d. *Special Holiday/Summer Tours.* These special tours are reserved for Treasury employees only and pre-arranged by the Curator's Office upon confirmation to the requesting employee. Employees are requested not to invite family/friends or have such non-employees show up for these tours. Family/friends are to be directed to partake of specific weekend tours (see a. above).

e. *Assistant Secretary (and above) Tours.* These are tours specifically requested by Treasury Assistant Secretary and higher level officials and may also include guided

tours for visiting foreign dignitaries with advance notification to both the USSS and Curator's Office.

f. *Informal Tours.* For any informal tour conducted by individual employees (for immediate family/friends), the employee is personally responsible for the conduct of their guests (and minor children) and must remain with them for their entire stay at Treasury. The Treasury Building is a working environment therefore visits to individual rooms may be limited to only hallway corridor areas.

g. All tours are subject to the following rules:

(1) Guests must be under escort by one (or more) Treasury employee or docent at all times. Escort responsibilities include keeping tour groups together and preventing the separation of any person(s) from the group.

(2) Visitors coming for a tour of the building shall be advised before each tour commences that photographic and recording devices may NOT be used inside the Main Treasury building. Treasury employees and docents shall advise and ensure visitors' cell/camera phones are turned off during tours.

(3) Additionally, NO photographs are permitted to be taken showing the adjacent White House property and grounds from within the Treasury building or showing security access control features or Secret Service personnel inside the building. This may subject the Treasury employee to possible disciplinary action.

(4) Interns (whether paid or unpaid) may NOT serve as tour escorts.

(5) Visitors shall be restricted from loitering in any work spaces to avoid perusing work areas, desks, open security containers, etc. and must be steered clear of all activated computer screens.

(6) Visitors shall be advised to keep the volume of any talking to a minimum so as not to disturb the work of Treasury employees.

(7) Visitors shall be managed in such manner that they are NOT able to listen in on business conversations conducted in rooms with open hallway doors.

(8) Visitors on weekday tours must NOT obstruct normal employee hallway traffic; minor children are NOT to run in the hallways.

16. Property Passes

Personnel removing property from the Main Treasury and Annex Buildings must have a DO Property Pass, DO F 70-03.10, (no carbon required) form completed and signed by the person removing the property and his/her administrative contact for the responsible office. Copies 1 and 2 shall be handed to the Secret Service officer at the exit upon removal of the property; the USSS officer shall sign off (in block 12) and keep copy 1 and forward copy 2 to the Personal Property Services Branch, Facilities Services. Copy 3 shall be retained by the administrative contact pending return of the property (as applicable). When the property is returned, the date of return shall be indicated in block 10 on the property pass. The annotated Copy 3 shall then be forwarded to the Personal Property Services Branch. Blank forms may be obtained from Facilities Services in Room 1150 Treasury Annex. Individual offices shall keep their signature approval authorization list of persons who may sign property passes current with the Office of Security Programs as changes are necessary. OSP will provide USSS updated authorization lists.

17. Press Representatives

As requested by the Office of Public Affairs (OPA), press representatives may be badged for unescorted access to the Main Treasury Building (MTB) to facilitate coverage of Treasury functions and related activities during official business hours, Monday through Friday, subject to the following procedures.

a. *Office of Public Affairs.* OPA will receive and approve formal access requests (on official letterhead) from respective news media for each press representative assigned to cover Treasury functions and related activities. OPA will vet each news media access request and provide individual news media representatives a Work Order/Pass Application form (TD F 15-05.1888). OPA will review each TD F 15-05.1888 for completeness and provide same to OSP. Upon notification from OSP that the USSS vetting is successful, OPA will coordinate press representatives meeting their scheduled appointment for fingerprinting and photographing. Individual press representatives that USSS disapproves for badged access will be so notified by the USSS as to why they have not been approved for access; their news organizations will not be informed as to the rationale except that access is denied.

b. *Office of Security Programs.* OSP will review and provide completed TD F 15-05.1888 to the USSS in order for them to conduct standard vetting checks in the same manner in which they determine MTB accessibility for all employees, contractors and visitors. Upon notification from the USSS of successful vetting, OSP will notify OPA and assign news media representatives an appointment for fingerprinting/photographs.

News media representatives who fail to meet scheduled appointments will need to be reassigned a new appointment (to be coordinated by OPA); this includes OPA submitting each request through the MTB appointment system.

c. *Official Rules Governing Press Representatives Access to the Main Treasury Building (TD F 15-05.20).* A TD F 15-05.20 (see Attachment 2) must be signed by each press representative approved for unescorted access to the MTB. The form includes the name, signature, date and employing press agency. Signed forms will be maintained on file in the OSP for the duration of the press representative's assignment covering the Treasury Department on behalf of their employing press agency. Failure to abide by the official rules governing press representatives access to the MTB will result in termination of the unescorted access privilege.

d. *Main Treasury-Approved Unescorted Access.* Approved unescorted access by press representatives is limited via the (North) Pennsylvania Avenue entrance and further to the 2nd floor northeast elevator and stairwell at that location to reach the "Press Office" in Rooms 1040/1044, MTB, nearest 1st floor restrooms and 1st floor Vault Cafe. Authorized unescorted access also applies to events held in the 2nd floor Treasury Cash Room and the Media Room (4121) when press representatives are officially invited to those particular events or activities by the OPA. Upon entering the MTB all unescorted press will proceed directly to the above rooms.

e. *Restrictions.* Access to or through the Treasury Annex is not permitted except for entry/exit after official business hours and in coordination between OPA and OSP and for press access to cover special news events and holidays/weekend activities. Additionally internal hallway corridors, office rooms and upper/lower level (basement, and 2rd through 5th) floors unrelated to press coverage of Treasury functions, activities and scheduled meetings is not authorized and requires an appropriate Treasury employee escort using the most direct route. Mobility-impaired press may use the 15th street entrance/exit and elevators, as necessary. No other stairways or elevators will be used, except as directed by Treasury Department officials during actual emergencies and/or scheduled evacuation drills. Access badges are U.S. Government property and are NOT authorized to be used for identification purposes at another Federal department or agency, or at any state, local, tribal or private organization. When employment ends or upon re-assignment from Treasury with your sponsoring press agency, this unescorted access badge privilege automatically expires and you are required to surrender your Treasury press badge by either turning it in to the OPA or dropping it in the slot at the (North) Pennsylvania Avenue, NW entrance/exit.

f. *Displaying Access Badges and Conducting Business.* While inside the MTB, press representatives are required to visibly display their press access badge on a lanyard, chain, or clip at all times in the same manner as employees, i.e., ***above the waist***. All press activity will be conducted in the space provided for that purpose and not Treasury hallways and corridors. Press representatives are required to follow and comply with all established Treasury Department instructions and procedures during authorized access to the MTB. This may include, but is not necessarily limited to sign-in/out policies; information and physical security screening procedures; and restrictions on use of personal digital assistants or blackberry communication devices, cellular phones and two-way pagers. Photographic and recording equipment may only be used as approved in writing by the OSP and such requests shall be made by press representatives via the OPA.

18. Limitations on Interns

a. *Interns.* Interns are highly qualified appointees who enjoy the benefits and challenges of developmental opportunities available in the Federal Government. DO/bureaus benefit as such appointments play important roles, for example, in strategic recruitment, streamlined hiring, and succession management. Interns include both paid and unpaid individuals yet their work has limitations with respect to that performed by employees, detailees, consultants and contractor personnel.

b. *Access to Classified and/or Sensitive Information.* Unless special arrangements are made for an intern to be investigated for access to classified information and issued a security clearance, interns may not work with, handle, process, and store, photocopy, or participate in the destruction of classified information nor should classified information be made available to them in open view or discussed in their presence. Access to sensitive information by interns may be permitted depending on restrictions applicable to such information and the specific requirements of the internship.

c. *Building Access for Interns.* Interns may have unescorted access to the Treasury Complex during normal business hours (7:00 AM through 6:30 PM, Monday through Friday). After hours and on weekends/holidays, interns must be either escorted by a DO badge-holder or the DO badge-holder must be present in the office to which the intern is going (and confirmed via phone call with the DO badge-holder). Keys to office work areas are not issued to interns. Interns themselves are not authorized to escort visitors but may assist in directing visitors and guests to appropriate locations to attend an event or meeting, briefing,

ceremony, or other commemorative event in or on the grounds of the Treasury Complex. All interns are required to submit the Work Order Pass Application form and will be scheduled by OSP for fingerprinting by USSS. Interns assigned to work in the Treasury Complex can be issued a DO access badge as determined by the OSP.

19. Security Screening of Persons, Packages, Mail and Deliveries

a. *Routine Security Screening.* Employees, detailees, contractors, consultants and visitors entering the Treasury Complex are required to pass through the metal detector (magnetometer) at each building entrance as part of the security screening process. All individuals, hand-carried items and packages are subject to x-ray screening and/or visual inspection by the USSS officer at the point of entrance.

b. *Modified Access Control.* **Senior Treasury officials whose office is located in the Treasury Complex and who have an "official" photograph displayed at the entrances, (to assist USSS officers in identifying these on-site officials) are exempt from routine security screening.** Persons accompanying these officials, however, must present their DO access badge and undergo appropriate security screening.

c. *Essential Personnel.* Only in the event of an emergency, as directed by the USSS, may designated essential personnel (as notated by the red indicator on the bottom of the HSPD-12 access badge), be allowed access into a restricted area. Such employees are subject to routine security screening for access to the Treasury Complex at all other times.

d. *Equipment, Furniture, Supplies and Foodstuff.* All deliveries of equipment, furniture, supplies and foodstuff are screened by USSS before being allowed on the premises. All such deliveries must be scheduled in advance for delivery to the southwestern moat area (Main Treasury) or via the H Street alleyway (Annex) in coordination with the Office of Facilities and Support Services.

e. *Personal Deliveries.* DO employees and contractors are not permitted to schedule personal deliveries of food items, flowers, gifts, etc., for receipt at or arrange to meet delivery personnel near the Treasury Complex. This is intended to prevent introduction of hazardous items by individuals intent on causing injury/damage via seemingly innocent items by unwitting employees/contractors in the same

manner as the flying public being advised to not carry items from strangers on aircraft. Further, USSS officers will not accept such deliveries on behalf of DO employees or contractors. Personal items, gifts, and food items either purchased locally or brought from home may be carried into the Complex by DO employees and contractors after routine security screening. (See item f. below).

f. *Non-Circumvention of Security Screening Procedures.* DO employees and contractors are prohibited from accepting delivery of solicited products from courier/messenger services or commercial firms as a means of circumventing USSS procedures designed to screen all incoming deliveries and safeguard personnel employed in, assigned to, or visiting/meeting Treasury officials in the Treasury Complex. This includes employee/contractor bypassing USSS practices and procedures if receiving deliveries by meeting the courier/messenger service provider immediately outside, across from, adjacent to, or within walking distance of the Complex. Circumvention of security screening procedures may result in badge access privilege restrictions or loss of the loss of badge access privileges to enter the Complex.

g. *Communications Security.* In general, keying material (FORTEZZA or KOV-14 cards used to conduct secure phone calls) may be subject to normal security x-ray screening without harmful effect to the material. In special circumstances, however, national security material may be exempt from x-raying. Exceptions must be approved in advance by the Director, OSP on a case-by-case basis. The material is still subject to visual inspection by the USSS officer.

20. Access to Treasury Complex during Non-Business Hours

After regular business hours and on weekends/holidays, only the Alexander Hamilton Place and Madison Place entrances are accessible. DO access badge-holders must sign in (and out) on the USSS Employee After-Hours Log-in Book upon entering and exiting the Treasury Complex. The badge-holder must identify their room and telephone number so USSS will be able to locate them in the event of an emergency. DO access badge-holders must use the badge reader feature on their badge and their PIN number to open the turnstile. Weekend/holiday contractor access requests must include each person's name, date of birth, social security number, vehicle description (and tag/State number when used to park in USSS-controlled parking areas) along with the name of the DO badge-holder providing escort. This information (see Attachment 1) must be provided on TD F 15-05.16 (Request for After-hours Access to the Main Treasury Complex) available at http://thegreen.treas.gov/policies/Forms1/Request%20for%20After-hours%20Contractor%20Access%20to%20the%20Main%20Treasury%20Complex.pdf (revised

October 2011) and be received by OSP **no later than 1:00 PM** the day prior in order for it to be approved and forwarded to USSS. Earlier versions of this form may no longer be used. DO employees must use the on-line form at http://thegreen.treas.gov/policies/forms/Pages/TreasuryAppointment.aspx to request access for family members and visiting guests. Note that all visitors to the Main Treasury Complex must be escorted at all times by the DO employee.

21. Secure/Sensitive Areas

a. *Standard Operating Procedures.* Access to secure/sensitive areas must be specifically approved by the appropriate security authority. When a bearer's PIV card is required for access to secure/sensitive work areas, authorized employees/contractors shall individually use their badge for access. Piggy-backing off another's access badge to gain entry and/or using facial recognition to allow another person to access secure/sensitive areas ***without first verifying*** they are wearing their PIV badge or "FORGOTTEN PASS" is prohibited. Standard operating procedures for the particular location shall be prescribed (in writing) for admittance, e.g., programming the bearer's DO access badge for entry, sign in/out, escort requirements, etc. Access to the exterior roofs of the Main Treasury and Annex Buildings is restricted to authorized personnel in direct coordination with USSS and may require a USSS escort.

b. *Recordings and Photographs.* Video/audio recordings and photographs are not permitted in secure/sensitive areas including photos taken from inside the Main Treasury Complex showing adjoining external areas not otherwise available to or observable by the general public. Any devices such as palm pilots, cellular phones, blackberries, pagers, cameras, etc., must be stored in (the provided) key-operated locker spaces until the individual exits secure and/or sensitive areas. Images of lobby security access controlled areas, security operations and personnel employed therein are prohibited.

c. *Treasury Secure Data Network.* Office space housing Treasury Secure Data Network (TSDN) computer terminals must be deadbolt-locked and the individual must log off the computer when the area is not occupied. Employees working in rooms with TSDN computers, including those employed in adjoining rooms connected by internal hallway must have at least a security clearance level of "Secret" issued by the OSP.

d. *Unlocking Rooms.* DO employees are issued and responsible for using their key to open the corridor hallway door to their office. During official business hours, OSP may be contacted to unlock hallway doors when it can be positively determined that a particular employee is assigned to specific office space. Neither OSP nor USSS will unlock a hallway door in the Treasury Complex where the employee does not work therein and/or has no official business.

22. Demonstrations, Security Incidents and Treasury-sponsored Events

a. *Demonstrations.* The National Park Service and/or the Metropolitan Police Department of the District of Columbia are responsible for issuing permits for public demonstrations in the vicinity of the White House and the Treasury Complex. Treasury does not issue permits for or otherwise authorize public demonstrations within the fenced perimeter areas adjoining Pennsylvania Avenue, NW, Fifteenth Street NW, Hamilton Place, NW and the former East Executive Avenue.

b. *Fifteenth Street, NW.* In accordance with Treasury Order 100-19, "Fifteenth Street Safety and Security," persons or entities are prohibited from conducting any business, including, but not limited to, vending on the sidewalk that is adjacent to the Main Treasury Building and its adjoining grounds.

c. *Emergency Procedures.* USSS may implement emergency procedures when necessary to safeguard DO personnel, visitors, property, information and facilities by closing particular entrances/exits because of a "security incident". Examples might include, but are not limited to, suspicious or dangerous activities occurring or unattended parcels and packages found on or near the Treasury Complex. During security incidents, the USSS official-in-charge will approve all global e-mail from emergency preparedness personnel to all DO LAN users, alerting them to particular entry/exit closings and provide an "all clear" notice when normal activities may be resumed.

d. *Treasury-sponsored Events and Special/Temporary Access Badges.* DO might schedule and host commemorative Treasury-related celebrations and other events that are open to only DO badge-holders and/or invited guests. For outside Treasury events, USSS screening may occur at the outermost fence or designated entry and/or controlled perimeter areas. For internal Treasury events, normal or modified access controls will apply depending on conditions as determined by USSS. During national level events (such as inaugural celebrations and during

transition periods), one-day inaugural badges may be issued to DO employees and their invited guests in lieu of honoring the normal access badge for the event. During transition periods temporary badges may be issued to on-boarding/interim officials requiring access to the Treasury Complex pending their final status. Such persons hired as DO employees will then be processed for normal access badges by OSP.

23. Regular, Express/Overnight Mail and Couriers

a. *US Postal Service Mail.* The United States Postal Service (USPS) irradiates all incoming mail for U.S. Government agencies/departments. USPS express/overnight and regular mail, and GSA-approved commercial carrier service mail destined for DO employees in the Treasury Complex is screened by USSS off-site for security concerns. In lieu of direct delivery, DO employees in satellite office locations should have incoming mail delivered to the Treasury Complex to ensure appropriate mail screening.

b. *Off-site USSS Mail Screening.* The USSS establishes and executes security practices and procedures for access to the Treasury Complex in coordination with the Director, Office of Security Programs (see Chapter VII, Section 1, TD P 15-71). Accordingly, all U.S. Postal Service and GSA-approved overnight and routine carrier mail and packages are now remotely screened off-site by the USSS. This is to ensure such items are not injurious to employee recipients before arriving at the Main Treasury Complex. When the above mail items are determined to be safe by the USSS screening procedures, the material items are transported to the on-site DO Mail Room for sorting and internal distribution.

c. *Couriers.* Couriers with proper identification from Treasury bureaus and other agencies making routine deliveries to the Treasury Complex will generally be badged for access. Courier carried mail and packages from known classified sources are exempt from being opened and screened. Couriers, however, are subject to normal pass-through the magnetometer and x-ray screening.

24. Carrying Firearms

USSS officers provide 24-hour armed security within the Treasury Complex. USSS may approve, on a case-by-case basis, other outside law enforcement officials carrying a firearm in the Treasury Complex upon a USSS official's determination that the duties of the law enforcement official warrant being armed and authorizes same. USSS directives require a 100%

identification check. In all other instances, other agency/department law enforcement officials must check their firearm at the USSS access control point and retrieve it upon leaving the Treasury Complex. Routine magnetometer and x-ray screening applies to non-USSS and law enforcement officials as for DO employees, bureaus, detailees, contractors, consultants and visitors with appointments.

Attachment 1

Request for After-hours Access to the Main Treasury Complex

Main Treasury Annex (Check applicable) Rooms and description of work: (List rooms/areas, roof, etc.) _____

Dates: _____ (from/to) Times: _____ (from/to) Treasury Escort Name and/Phone: _____

Last, First, In. Name Company/Office Country of Birth DOB SSN Vehicle/Tag/State

Sample for Display Purposes Only
Use form posted at
http://thegreen.treas.gov/policies/Forms1/Request%20for%20After-hours%20Contractor%20Access%20to%20the%20Main%20Treasury%20Complex.pdf

Comments:

Office of Security Programs approval: _____ Date: _____ Page ____ of ____

Notice: The information requested is protected by the Privacy Act, 5 U.S.C. 552a which requires that Federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that the authority for soliciting your Social Security Number (SSN) is Executive Order 9397 which authorizes agencies to solicit SSNs for use as identifiers for administrative purposes. This form will be used as a means to provide access to the Main Treasury and Annex buildings. Providing the information requested, including the SSN, is voluntary, however, if some or any part of the requested information is not provided, the effect will be that you will not be allowed after-hours access to the Main Treasury Complex.

TD F 15-05.16 (Revised Oct 2011)

Attachment 2

OFFICIAL RULES GOVERNING PRESS REPRESENTATIVES ACCESS to the MAIN TREASURY BUILDING

You have been approved for unescorted access to the Main Treasury Building (MTB) to facilitate press coverage of Department of the Treasury functions and related activities, Monday through Friday. This includes meetings with senior Treasury officials as arranged or scheduled by the Office of Public Affairs (OPA). The following access requirements pertain to all press representatives.

- Only the (North) Pennsylvania Avenue entrance will be used to enter/exit the MTB during official business hours. The 2nd floor northeast elevator and stairwell at that location will be used to reach the "Press Office" in Rooms 1040/1044, MTB. Upon entering the MTB all unescorted press will proceed directly to those rooms. Access to or through the Treasury Annex is off limits, except for entry/exiting the MTB after official business hours and in coordination between OPA and the Office of Security Programs (OSP). The same coordination is required for press access to cover special news events and holidays/weekend activities.

- While inside the MTB you are required to visibly display the press access badge on a lanyard, chain, or clip at all times. You are authorized unescorted access to the nearest 1st floor restrooms near the Press Office and the 1st floor Vault Café. You are also authorized unescorted access to attend events held in the 2nd floor Treasury Cash Room and the Media Room (4121) when officially invited to those particular events or activities by the OPA.

- You are NOT authorized unescorted access to internal hallway corridors, office rooms and upper/lower level (basement, and 2rd through 5th) floors unrelated to press coverage of Treasury functions, activities and scheduled meetings. Access to any of the unauthorized areas require a Treasury employee escort and must be by the most direct route possible. The central entrance, exit area and elevators on the 15th Street side of the MTB may only be used by individuals with impaired mobility. No other stairways or elevators will be used, except as directed by Treasury officials during actual emergencies and/or scheduled evacuation drills.

- On-site press representative's business will be conducted in space provided for their use and not conducted in Treasury hallways or corridors. You are required to follow and comply with all established Department of the Treasury instructions and procedures during authorized access to the MTB. This may include, but is not necessarily limited to sign-in/out policies; information and physical security screening procedures; and restrictions on use of personal digital assistants or blackberry communication devices, cellular phones and two-way pagers. Photographic and recording equipment may only be used as approved by the OSP and such requests shall be made via the OPA.

All Treasury access badges are U.S. Government property and are NOT authorized to be used for identification purposes at another Federal department or agency, or at any state, local, tribal or private organization. When employment ends or upon re-assignment from Treasury with your sponsoring press agency, this unescorted access badge privilege automatically expires and you are required to surrender your Treasury press badge by either turning it in to the OPA or dropping it in the slot at the (North) Pennsylvania Avenue, NW entrance/exit.. Failure to follow the above rules will result in the termination of your MTB access.

Printed Name _____ Employing Press Agency _____
Signature_____ Date _____

TD F 15-05.20 Copy received: _____ (Initial)

Attachment 3

PIV ISSUANCE PROCEDURES FOR CONTRACTOR PERSONNEL

SUBJECT: Policies for a Common Identification Standard for Federal Employees/Contractors
It is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors.

Contractors that require access to the Main Treasury Complex or Department Offices (DO) computer systems are required to follow the common identification standard. **Contractors assigned for 210 days will be issued a PIV access badge (card).**

CORs/COTRs will collect and validate the correctness of the data (Work Order Pass Application form TD F 15-05.18 (commonly referred to as 1888), before forwarding to the Office of Security Programs (OSP), Treasury Annex Room 3180 (attn: Camellia Murdock).

Requirements for processing contractors: Work Order Pass Application.

- Application must be filled out completely and legibly. Incomplete or illegible application forms will be returned to CORs/COTRs.
- Application must include Period of Performance (from XX date /to XX date).
- Request for 24/7 access must include the justification of valid need.
- Attach a legible copy of Certificate of Birth of a U.S. Citizen Born Abroad, Certificate of Naturalization, Lawful Permanent Resident Alien (green) card or divorce decree, name change document if applicable.
- Work Order Pass Application forms expire 30 days from the date of contractor signature.
- The Secret Service Appointment Center (SSAPPT) will not process expired application forms; a new one must be generated.

Requirements for processing contractors: PIV Access Badge issuance requirements.

- Contractors must possess a Treasury (DO) email address and a Treasury Enterprise Directory Identification Number (TEDSID) that is associated with each account.
- Applications submitted to OSP without an email/TEDSID will be destroyed.
- CORs/COTRs shall submit EEE on-boarding information (badge only) for contractors who will not access DO computing systems but require access to DO facilities i.e., housekeeping and maintenance personnel.
- Contractor email addresses must match their legal name (first and last) as indicated on corresponding identity documents.

Requirements for processing contractors: Processing Time

- Estimated access badge issuance is within 6 to 8 weeks. Adherence to these procedures will ensure the process is completed within this time-frame.
- CORs/COTRs and contractors will receive sponsorship notification via their email account containing information for enrollment.
- COTRs and contractors will receive access badge pickup notification after all processes are completed.

Requirements for processing contractors: Enrollment and Access Badge Pickup

- Contractors who work in the Treasury Complex shall enroll and pickup their PIV access badge in Room 1016 (enter through hallway corridor at Room 1015 and turn right), Main Treasury.
- Contractors assigned to 1801 L Street, or 1750 Pennsylvania Avenue, Metropolitan Square etc., or location other than Main Treasury shall enroll and pickup their access badge at the General Services Administration (GSA) Building, 1800 F Street, NW, and Room G042.

This process will avoid the need for the CORs/COTRs/supervisors to make appointments for contractors to access the Treasury Complex after their PIV access badge has been issued.

- CORs/COTRs or contractors will receive automated email messages from HSPD12Admin@usaccess.gsa.gov (not from OSP) with pickup instructions.
  - The email should be printed as it contains their PIN code required to activate the PIV access badge.
  - It is ***vital*** for each contractor to bring the email notice with him/her to their access badge pickup appointment.
- CORs/COTRs and/or supervisors must then make visitor appointments for each applicant to access the Main Treasury Complex and to have the PIV access badge encoded for physical access to Main Treasury by the Secret Service in Room 1016, Main Treasury.
- Pass Applications processed by Secret Service will expire 90 days from the date of the contractor signature on Work Order Pass Application.
  - Secret Service Pass and Lock (SSPASS) will not encode PIV access badges beyond the 90 day expiration date.
  - Applications are returned to OSP for destruction. Notification is not sent to the COR/COTR.
- Contractors are required to store PIV access badge in the protective sleeve provided at time of access badge pickup. Self-purchase of optional sleeves is discouraged to ensure the protection/safeguarding of personnel identifiable information and avoid damage to the access badge.

Chapter VII Section 2 **Security Access Controls for Departmental Offices Leased Facilities** Updated 5/16/14

1. Introduction

The Departmental Offices (DO) leases space in commercial buildings in the general vicinity of the Main Treasury and Annex Buildings in Washington, DC. Unlike the Main Treasury and Annex Buildings, DO-leased spaces are not part of the White House Complex and the Uniformed Division, U.S. Secret Service does not provide security or related services at DO leased space.

Access controls in DO leased buildings are initially governed by the Federal Protective Service (FPS) and the General Services Administration (GSA). GSA coordinates security assessments of proposed lease spaces and implements appropriate measures based on minimum security levels established for each location (see Chapter V, Section 1). FPS conducts security evaluations of commercial facilities housing U.S. Government employees; investigates incidents, responds to alarms, and in some cases has uniformed officers or contract guards at the building entrance(s). Supplemental security controls not already included in lease arrangements may be requested by individual Building Security Committees at each facility and are subject to availability of funds. DO tenants may also impose additional security controls within their immediate office spaces to regulate access by official visitors and/or service providers to particular work areas.

2. Building Security Committees and Security Points of Contact

Building Security Committees in DO-leased facilities shall include DO security, facilities management and emergency preparedness representatives. Additional members shall be designated by each Assistant Secretary-level component whose employees are housed in commercially leased facilities. This is to ensure their interests and concerns are represented and to have participation by on-site DO employees. A primary and alternate designee from one or more on-site offices shall be identified to the Director, Office of Security Programs (OSP). The Director, OSP shall also be notified of any changes in designees as employees depart, retire or transfer within the organization.

Such designees will serve as the Security Point of Contact (SPC) and liaison for non-technical inquiries and administrative support with OSP security officials. The same individuals may also be contacts for facilities management and emergency preparedness functions. SPC duties include, but are not necessarily limited to, alerting security officials about needed security container repairs, combination changes and reporting problems with alarms, doors, locks, keys,

etc., providing information on suspicious persons, phone calls, packages or activities, requesting and issuing card access keys/cards/fobs, and scheduling sensitive but unclassified waste collection/destruction.

3. DO Access Badges

DO access badges for the Main Treasury Complex are also issued to DO employees in leased facilities. The badge may need to be shown to the FPS, GSA or other uniformed guard personnel at the front entrance to commercially leased facilities. Wearing the DO access badge within DO-leased space is encouraged especially within DO leased areas housing numerous employees and multiple DO offices. DO employees in leased space have ready access to the Main Treasury Complex but are not authorized to make appointments for others to have access to the Main Treasury or Annex Buildings.

4. Forgotten and Lost Badges

DO access badge-holders (including detailees and consultants) who have forgotten their badge may be required to present alternate photo ID, e.g., driver's license, U.S. passport, DO ID, or other identification to enter DO leased facilities. DO employees working in leased facilities who have lost their access badge must report the loss in writing (e-mail will suffice) to OSP within 24 hours. There is a 10-day waiting period for a lost or stolen badge to be recovered. If the badge is not recovered, OSP will notify the individual's supervisor, the U.S. Secret Service Pass office and Human Resources (HR). HR must then re-initiate the Personnel Identification Verification process for a DO employee, detailee or consultant's replacement badge to be issued.

5. Security Screening of Persons, Packages and Deliveries

All individuals, hand-carried items and packages are subject to screening and/or visual inspection at the point of entry to DO-leased facilities. Deliveries of equipment, furniture, supplies, mail and other items should be addressed to Main Treasury for screening and subsequent delivery to DO-leased offices.

Deliveries of supplies, equipment and furniture (via the Treasury Moat and/or Annex loading dock) for eventual transport to DO-leased facilities must be submitted before 2:00 PM the day before the delivery. Contact the Office of Facilities and Support Services for assistance in scheduling deliveries to the Complex. That office is responsible for relaying delivery information and coordinating with the Uniformed Division, U.S. Secret Service.

DO employees are discouraged from scheduling personal deliveries of food items, flowers, gifts, etc., for receipt in DO-leased space. Uniformed FPS, GSA or contract guards are not authorized and will not accept deliveries on behalf of DO employees.

6. Access After Regular Business Hours

Outside of normal business hours and on weekends DO access badge-holders must sign in/out on the After-Hours Log upon entering and exiting DO-leased facilities. Where applicable, the badge-holder should indicate their room and telephone number so they may be located inside the building the event of an emergency by responding personnel.

7. Video/Audio Recording and Photographing

Photographs of security-controlled areas into DO controlled space are prohibited especially where features or equipment may provide information not otherwise accessible to the general public. Ceremonial or commemorative type functions, for example, award presentations, retirement celebrations and similar programs in interior spaces, however, may be photographed in support of such events.

8. Demonstrations and Security Incidents

The National Park Service and/or Metropolitan Police Department of the District of Columbia are responsible for issuing permits for public demonstrations in the vicinity of the White House and Treasury Complex. DO employees in leased facilities receive notifications via the DO LAN about emergency procedures affecting the Main Treasury Complex that may include, but are not limited to, suspicious or dangerous activities occurring or unattended parcels/packages found on or near the Treasury Complex. Global email from emergency preparedness personnel also alert DO LAN users to particular Treasury Complex entry/exit closings and provide an "all clear" notice when normal activities may be resumed.

9. Regular, Express/Overnight Mail and Couriers

The United States Postal Service (USPS) irradiates all incoming mail for U.S. Government agencies and departments. USPS express/overnight and regular mail, and GSA-approved commercial carrier mail destined for DO is screened for manifold security concerns. To ensure mail destined for delivery to DO-leased office locations is screened it should be directed in care of the Treasury mailroom. Courier deliveries of unclassified but sensitive mail should also be addressed in care of the Treasury mailroom for screening rather than received directly in DO-leased offices.

Chapter VII
Section 3

Departmental Offices
Security Clearance Verification

Updated
6/17/11

1. Office of Security Programs Responsibility

As the issuing authority for Departmental Offices (DO) collateral (Top Secret, Secret and Confidential) security clearances, the Office of Security Programs (OSP) is responsible for verifying and passing security clearance information on individuals authorized access to classified information. Whenever access to classified information is required at other bureaus, agencies/departments or activities, OSP will pass security clearance verification to the necessary recipient(s), as requested. Individuals may **NOT** pass their own security clearance.

2. Treasury Department Form TD F 15-03.6

Individuals for whom OSP holds a security clearance shall notify OSP personnel security officials (at least 24 hours in advance) of all classified meetings/briefings where security clearance verification is required. Such individuals shall complete TD F 15-03.6, Request for Security Clearance Verification (see Attachment 1), available on the OSP website at http://intranet.treas.gov/security/forms/TDF15-03-6.pdf and forward to OSP via e-mail or fax (202) 622-2429. Where individuals attend routinely scheduled classified meetings or briefings, OSP will certify the security clearance for up to one year.

For questions concerning collateral security clearance information within the DO, the offices of the Inspectors General, et al., contact OSP personnel security specialists on (202) 622-1112.

3. Sensitive Compartmented Information

Individuals who need their access to Sensitive Compartmented Information verified must contact the Office of Intelligence and Analysis on (202) 622-1837.

Attachment 1

Department of the Treasury
Request for Security Clearance Verification

For security clearance information to be verified (passed) as expeditiously as possible, the following data must be provided to Treasury/bureau personnel security specialists holding your clearance certification.

Employee Name: _____ Date of Request: _____

Date of Birth: _____ SSN: _____ Office Phone: _____

Bureau/Agency/Department requiring security clearance verification; phone/fax:

_____

Point of Contact/Sponsor Name: _____

Contact/Sponsor's Phone and Fax Numbers: _____

Meeting/Visit Dates: (from) _____ (to) _____ Permanent Certification ☐Yes ☐No

Location(s) (as applicable): _____

Purpose: _____

_____

Please allow 24 hours from personnel security specialists' receipt of this form for security clearance information to be passed to recipient(s).

Notice: In compliance with the Privacy Act of 1974, 5 U.S.C. § 552a the authority for soliciting your Social Security Number (SSN) is Executive Order 9397 which authorizes agencies to solicit SSNs for use as identifiers for administrative purposes. Your SSN is needed to keep records accurate, because other people may have the same name and birth date. This information will be used as a means of verifying your security clearance to Treasury bureaus and other agencies/departments. Information will be transferred to appropriate Federal, State, local or foreign agencies when relevant to civil, criminal, or regulatory investigations or prosecutions; or pursuant to a request any other agency in connection with hiring or retention of an employee, the issuance of a security clearance, the investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit. Disclosure of the information is voluntary. If some or any part of the requested information is not provided, the effect will be that the processing of your request for security clearance verification will be impeded or possibly result in the denial of access to classified information.

TD F 15-03.6

Chapter VII **Procedures for Issuing Courier Cards** Updated
Section 4 **and Credentials in the Departmental Offices** 5/13/14

1. Office of Security Programs Responsibility

The Office of Security Programs (OSP) has responsibility for policy development regarding issuance, management, maintenance of Department-wide courier cards and credentials. OSP is the issuing authority within the Departmental Offices for both courier cards and credentials and may delegate the authority to Treasury bureaus to issue courier cards where the volume is significant. Treasury bureaus have responsibility for the issuance and control authority for credentials within their organizations.

2. Required Training

Employees issued courier cards and/or credentials must complete mandatory training developed by OSP available on-line at http://thegreen.treas.gov/programs/Pages/training.aspx. The training modules are listed under individual headings by topic, i.e., "Courier Authorization", "Courier Training", Hand Carrying Classified Information", "Modes of Transport for Couriering", "Credentials Training", etc.

3. Self-Certification.

Upon completion of the above training, DO employees must self-certify (via the DO LAN to OSP) that they have completed the training and understand their responsibilities with respect to having a courier card and/or credentials issued to them. The self-certification also applies to bureau employees for whom OSP issues a courier card and/or credential.

4. Misuse of Official Courier Cards and Credentials

Courier cards and credentials are only to be used for the conduct of official United States Government business. Use for non-official or personal reasons may constitute rationale for administrative and/or disciplinary action including temporary suspension, reassignment, revocation of official duties and responsibilities, or other penalties. Instances of inappropriate use involving senior Treasury officials shall be reported concurrently to the Director, OSP and the Office of Inspector General (OIG). The OIG in consultation with the Director, OSP shall determine whether an investigation is warranted and who will conduct it.

5. Issuing/Authenticating Authority

The DO issuing or authenticating authority for courier cards and credentials is the Director, OSP. This authority is delegable within OSP only.

6. Treasury Department Form TD F 15-05.12 (Request and Receipt for Courier Card

Requests for issuance of a courier card must be on TD F 15-05.12 (Request and Receipt for Courier Card). See also Chapter V, Section 6. The form is available on the OSP website at http://thegreen.treas.gov/policies/Forms1/Request%20and%20Receipt%20for%20Courier%20Card.pdf. See Attachment 1. Completion of the items on the form is self-explanatory and the form may be provided to OSP via the DO LAN or in hard copy. Upon receipt, OSP will obtain the employee's photo from the U.S. Secret Service, Pass and ID office. Each courier card will note the level of the employee's security clearance and/or access to Sensitive Compartmented Information, as appropriate, and be assigned a control number and dates of issuance and expiration. All such cards expire after 5 years on the calendar date of December 31st.

OSP will direct the employee to complete the required training and advise him/her about the requirement to self-certify having done so. OSP will notify the employee when the courier card is ready to be issued. Courier cards are generally issued in OSP at either 9:30 AM or 1:30 PM., Monday through Friday; other times may be arranged as warranted. At the time of issuance the employee will sign the receipt part of the TD F 15-05.12. Courier cards will not be issued to or receipted by other than the intended recipient.

7. Treasury Department Form TD F 15-05.14 (Request and Receipt for Official Credential

Requests for issuance of an official credential must be on TD F 15-05.14 (Request and Receipt for Official Credential). See also Chapter V, Section 5. The form is available on-line at http://thegreen.treas.gov/policies/Forms1/Request%20and%20Receipt%20for%20Official%20Credential.pdf. See Attachment 2. Completion of the items on the form is self-explanatory and the form may be provided to OSP via the DO LAN or in hard copy. Upon receipt, OSP will obtain the employee's photo from the U.S. Secret Service, Pass and ID office. Each credential will be assigned a control number and date of issuance. There is no expiration date and credentials may continue to be used provided they are undamaged over time and the photo is an acceptable image of the bearer.

OSP will direct the employee to complete the required training and advise him/her about the requirement to self-certify having done so. OSP will notify the employee when the credential is ready for signature. The credential will be laminated and affixed to the permanent case/holder.

Employees will be notified again when the credential is ready. At the time of issuance the employee will sign the receipt part of the TD F 15-05.14 to be maintained by OSP. Credentials will not be issued or signed for by other than the intended bearer.

8. Lost, Misplaced and Expired Courier Cards and Credentials

Lost or misplaced courier cards and/or credentials shall be reported to OSP in writing within 48 hours. Notification to the OSP may be made via the DO LAN, as appropriate describing the nature of the loss and likelihood of retrieval. In order to replace courier cards and/or credentials, a new TD F 15-05.12 or TD F 15-05.14 must be completed.

9. Procurement of Badges/Shields

Within the Departmental Offices, badges/shields may only be commercially procured as authorized by the Director, OSP.

Attachment 1

Department of the Treasury
Request and Receipt for Courier Card

To be completed by requesting Supervisor

Employee Name _____ Date of Birth _____ SSN _____

Phone Number _____ Frequency of Courier Responsibilities _____

Treasury Bureau _____ Treasury Contractor _____

Requested Courier Level: Confidential ☐ Secret ☐ Top Secret ☐ SCI ☐
(Check only one)

Supervisor's signature _____ Date _____

To be completed by Special Security Officer (for SCI only)

Special Security Officer's signature _____ Date _____

To be completed by Security/Issuing Office

Employee Reviewed Courier Training Module: Yes ☐ No ☐

Clearance Verified: Yes ☐ No ☐

Assigned Courier Card Number _____ Expiration Date _____

To be completed by Courier

Receipt is hereby acknowledged for the above courier card. I understand the courier card must be turned in to the security/issuing office when my services as a courier are no longer required.

Courier's Signature _____ Date _____

Notice. The information requested is protected by the Privacy Act, 5 U.S.C. 552a which requires that Federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that the authority for soliciting your Social Security Number (SSN) is Executive Order 9397 which authorizes agencies to solicit SSNs for use as identifiers for administrative purposes. This form will be used as a means to prepare and issue a credential. Providing the information requested, including the SSN, is voluntary; however, if some or any part of the requested information is not provided, the effect will be that you will not be issued a courier card or be authorized to hand-carry and deliver classified information.

TD F 15-05.12

Attachment 2

Department of the Treasury
Request and Receipt for Official Credentials

(To be completed by Requesting Office Director)

Employee Name: _____ Date of Birth: _____

SSN: _____ Job Title on Credential: _____

Justification for Official Credentials (description):

Signature of Office Director: _____

In acknowledging receipt of official Department of the Treasury/bureau credentials, I agree to surrender them to the Treasury/bureau issuing authority for accountability and appropriate voiding prior to the termination of my employment in the position in which they were duly authorized. I have been advised that these credentials are only for the conduct of official Treasury/bureau business and that use for non-official or personal reasons may constitute rationale for administrative action.

I have been further advised to immediately report the loss, theft or misplacement of these credentials to the Treasury/bureau issuing authority.

Assigned Control Number _____

Employee's Signature _____ Date of Issue: _____

Issuing Authority: _____

Notice: The information requested is protected by the Privacy Act, 5 U.S.C. 552a which requires that Federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that the authority for soliciting your Social Security Number (SSN) is Executive Order 9397 which authorizes agencies to solicit SSNs for use as identifiers for administrative purposes. This form will be used as a means to prepare and issue a credential. Providing the information requested, including the SSN, is voluntary; however, if some or any part of the requested information is not provided, the effect will be that you will not be issued a credential.

TD F 15-05.14 (4/08)

Chapter VII Section 5

Check-list for Security Inspections and Surveys

Dated 6/17/11

This check–list is a sample for conducting day-time and after-hours security inspections and surveys with respect to protecting collateral classified information. It may be modified to include material pertaining to sensitive information or additional items unique to particular Departmental Offices/bureau needs. Copies may be used in assembling collected data for inclusion in official reports of security inspections and surveys or attached to such reports.

Inspection/Survey Item	Yes	No	Comment
Unsecured classified documents/burnbag(s).			Room/cubicle number: Highest classification level:
Safe(s) unlocked.			Barcode number: Highest level of accessible classified information:
OPEN/CLOSED used on safe.			
Unprotected COMSEC			
Security Container Check Sheet (SF702) not in use.			Room/cubicle number: Barcode number:

Inspection/Survey Item	Yes	No	Comment
Activity Security Check List (SF701) in secure room/approved open storage area.			Room number:
Clean work space (desk/safe) to thwart inadvertent disclosure/exposure of classified information.			
Classified processing equipment labeled/marked.			Type of equipment:
Classified/sensitive document cover sheets used.			
Classified documents properly marked. - overall - paragraphs/portions - subject line - declassification instructions			
User logged off IT systems.			
Hallway door unlocked on space with TSDN terminal.			Room/cubicle number:

Chapter VII Section 6

Schedule for Main Treasury Complex Entrances

Dated 12/5/13

Entrance	Location	Days	Hours	Access
South	Alexander Hamilton Place	Mon - Fri	7:00 AM to 6:30 PM	Departmental Offices (DO) and White House (WH) badge-holders. Appointments for Assistant Secretaries and above with escorts.
West	East Executive Avenue (Bell entrance)		24/7	DO and WH badge-holders. Appointments for Assistant Secretaries and above with escorts.
North	Pennsylvania Avenue	Mon – Fri	7:00 AM to 6:00 PM	DO and WH badge-holders. DO contractors on work orders. Visitors with Main Treasury Building (MTB) appointments.
Ramp	Alexander Hamilton Place (Gate at Moat)	Mon - Fri	7:00 AM to 6:30 PM	DO and WH badge-holders. DO contractors on work orders and Press/Media (carrying equipment) with appointments. All scheduled deliveries to the MTB.
B Door	Main Treasury Basement (West side Moat)	Mon - Fri	7:00 AM to 6:30 PM	DO and WH badge-holders. DO contractors on work orders and Press/Media (carrying equipment) with appointments. All scheduled deliveries to the MTB and motorcycle parking on Alexander Hamilton Place. For access to bicycle racks after hours contact Uniformed Division Command Post on (962-6700).

Secretary's Entrance	East Executive Avenue		Open when required	The Secretary, Deputy Secretary (and others as approved by the Secretary's Office).
East	Fifteenth Street (Handicapped Use and EXIT ONLY for DO and WH badge-holders.	Mon - Fri	7:00 AM to 6:00 PM	Entrance and Exit for mobility-impaired visitors (with MTB appointments), DO and WH badge-holders designated by Facilities and Support Services.
ANNEX West	Madison Place		24/7	DO and WH badge-holders. DO contractors on work orders. Visitors with Annex Building appointments.
ANNEX East	Annex Alleyway (Designated entrance to Annex for mobility-impaired persons).	Mon - Fri	7:00 AM to 6:00 PM	Mobility-impaired DO badge-holders as designated by Facilities and Support Services. Mobility-impaired visitors with Annex Building appointments.
ANNEX East (Loading Dock)	Alley to H Street	Mon - Fri	7:00 AM to 6:00 PM	All scheduled deliveries (through Facilities and Support Services) for Annex Building.

Chapter VIII
Section 1

Glossary of Security Terms

Updated
12/6/13

Access – (1) The ability and opportunity to obtain knowledge of classified information. An individual is considered to have access to classified information if he or she is admitted to an area where such information is kept or handled and security measures do not prevent that individual from gaining knowledge of such information. (2) A condition or equipment mode allowing authorized entry into a protected area without alarm by electronically or mechanically deactivating a sensor or sensors. (3) The ability and means to approach, store or retrieve data, or to communicate with or make use of a resource of an information processing system.

Access Approval – Formal authorization for an individual to have access to classified or sensitive information within a Special Access Program or a Controlled Access Program, including Sensitive Compartmented Information (SCI). Access requires formal indoctrination and execution of a non-disclosure agreement.

Access Control – (1) An aspect of security that utilizes hardware systems and specialized procedures to control and monitor the movement of individuals, vehicles, or materials into, out of, or within designated areas. Access to various points may be a function of authorization level, time, or a combination of the two. (2) The use of physical and procedural security controls to ensure only authorized individuals or items are given access to a facility or secure area.

Access Control System – An electronic, electro-mechanical, or mechanical system designed to identify and/or admit authorized personnel to the secure area. Identification might be based on any number of factors such as a sequencing of combinations, special keys, badges, fingerprints, signature, voice, etc. These systems are for personnel access control only and are not to be used for the protection of stored information or materials.

Access Eligibility Determination – A formal determination that a person meets the personnel security requirements for access to a specified type or types of classified information.

Accessioned Records – Records of permanent historical value in the legal custody of the National Archives and Records Administration; also known as permanent records.

Accreditation – The formal certification by a cognizant security authority that a facility, designated area, or information system has met Director of National Intelligence security standards for handling, processing, discussing, disseminating or storing classified information.

Adjudication – The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance.

Adjudicative Process – An examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk.

Adjudicator – A personnel security specialist who performs adjudications.

Administrative Inquiries – The preliminary collection and examination of available records, and the conduct of interviews of Treasury personnel to resolve sensitive allegations of misconduct, or incidents impacting the proper protection of classified or sensitive information, plans and programs.

Adverse Information – Information that adversely reflects on a person's integrity or character, that suggests that his or her ability to safeguard information may be impaired, or that his or her access to information may not be in the best interest of national security or the Treasury Department; for example, a history of drug abuse or criminal activity, whereas, issue information that is unrelated to character (such as foreign connections), while of adjudicative significance, is *not* derogatory information.

Agency – Any Executive agency as defined in 5 U.S.C. 105; any Military department as defined in 5 U.S.C. 102; and any other entity within the Executive Branch.

Agency Security Classification Management Program Data – Statistical data reported annually on Standard Form 311 including (1) the number of officials authorized to originally classify; (2) the annual volume (and levels) of original and derivative classification decisions; (3) the status of new, carried-over, and appeals for mandatory declassification review; (4) the number of pages subject to automatic declassification and systematic review; and (5) number of internal agency oversight reviews.

Alarm – An audible or visual signal that functions as an alerting mechanism.

Alien – Any person who is neither a citizen nor a national of the United States of America.

Alcohol and Tobacco Tax and Trade Bureau (TTB) – The Treasury bureau responsible for enforcing and administering laws covering the production, use and distribution of alcohol and tobacco products. TTB also collects excise taxes for firearms and ammunition.

Appeal – A formal request under the provisions of Executive Order 12968, Section 5.2., for review of a denial or revocation of access eligibility.

Applicable Associated Markings – Markings, other than those designating the classification level, that are required to be placed on classified documents and email. These include the "Classified by", "Derived from" lines and downgrading/declassification instructions, distribution limitations, etc.

Applicant – A person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

Asset – Any person, facility, material, or information that has a positive value to Treasury and which is controlled by that Department.

Authorized Adjudicative Agency – Any agency authorized by law, regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12968.

Authorized Classification and Control Markings Register – Also known as the "CAPCO Register", this is the official list of authorized security control markings and abbreviated forms of such markings for use by all elements of the Intelligence Community (IC) for classified and unclassified information.

Authorized Holder – Recipients requiring particular information in performance of a lawful, U.S. Government official mission purpose.

Authorized Investigative Agency – Any agency authorized by law, executive order, regulation or the Director, Office of Management and Budget (OMB) under Executive Order 13381 to conduct counterintelligence investigations or investigations of persons who are proposed for access to classified or sensitive information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

Authorized Person – A person, who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, has a need-to-know for the specific classified information in the performance of officials' duties, and has received contemporaneous training on safeguarding requirements for protecting classified information.

Automated Information System – Any assembly of computer hardware, software, firmware, or any combination of these, configured to accomplish specific information-handling operations, such as communication, computation, dissemination, processing, storage and retrieval of information. Included are computers, word-processing systems, networks, or other electronic information-handling systems and associated equipment. Management information systems are a common example of an automated information system.

Automatic Declassification – Declassification of information based solely upon the occurrence of a specific date/event as determined by the original classification authority; or the expiration of a maximum time frame for duration of classification; under EO 13526 and within the Treasury Department to a maximum of 25 years from date of origin. Automatic declassification "kicks in" on December 31st for information that reaches 25 years of age.

Background Investigation (BI) – An official inquiry into the activities of a person designed to develop information from a review of records, interviews of the subject, and interviews of people having knowledge of the subject.

Badges, Credentials and Shields – Credentials and badges/shields provide evidence of the bearer's authority when contacting the public and/or conducting U.S. Government business with Federal, State, local or foreign officials as authorized by law, statute or Treasury regulation. Credentials describe the specific authority and responsibilities of the bearer. Badges/shields are metallic emblems that convey the representative authority of the bearer.

Breach – The successful defeat of security controls resulting in a penetration of the system.

Building Service Contract Employees – Includes, but is not limited to, custodians, mechanics, electricians, plumbers, and guards.

Bureau of Engraving and Printing (BEP) – The Treasury bureau responsible for designing and manufacturing U.S. currency, securities, and other official certificates and awards.

Bureau of the Public Debt (BPD) – The Treasury bureau responsible for borrowing money needed to operate the Federal Government. BPD administers the public debt by issuing and servicing U.S. Treasury marketable, savings and special securities.

CAGE Code – The alpha-numeric designator assigned by the Defense Security Service to commercial firms participating in the National Industrial Security Program and which are authorized access to classified information at a specified level.

Card Access – A type of access control system using a card with a coded area or strip, on or inside the card, to activate a lock or other access control device.

Card Reader – An electronic device for reading information contained on an access card/key.

Caveat – An approved designator used with or without a security classification marking to further limit dissemination of restricted information.

Certification – The comprehensive testing and evaluation of the technical and non-technical IT security features, and other safeguards used in support of the accreditation process.

Certified TEMPEST Technical Authority – A U.S. Government employee who has met established certification requirements in accordance with the Committee on National Security Systems approved criteria and has been appointed by a U.S. Government department or agency to fulfill these requirements.

Change Key – A key that will operate only one lock or a group of keyed-alike locks, as distinguished from a master key.

Classification – The act or process by which information is determined to be classified information.

Classification Guidance – An instruction or source prescribing the classification of specific information.

Classification Guide – Guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Classification Levels – Top Secret, Secret and Confidential and appearing on classified information within parenthetical markings, i.e., (TS), (S), (C) and (U) for unclassified.

Classification Markings – Essential labels applied to classified documents to indicate the overall level of classification, which paragraphs and portions are classified (and those which are unclassified), the name or personal identifier or the originator, the reason for classification (or source(s) thereof) and the date or event for declassification.

Classified National Security Information or Classified Information – Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Classifier – An individual who determines and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on an approved classification guide or properly classified source.

Clearance – See "Security Clearance."

Clearance Certification – An official notification that an individual holds a specific level of security clearance and/or access approvals, authorizing the recipient of the certification access to classified information or material at that level.

Cleared Commercial Carrier – A carrier authorized by law, regulatory body, or regulation, to transport SECRET and CONFIDENTIAL material and has been granted a SECRET facility clearance in accordance with the National Industrial Security Program.

Closed Storage – The storage of classified information in properly secured General Services Administration-approved security containers.

Cognizant Security Authority (CSA): The single principal designated by a SOIC (see definition of SOIC) to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods, under SOIC responsibility.

Cohabitant – A person living in a spouse-like relationship with another person.

Collateral Information – National security information (including intelligence information), classified Top Secret, Secret, or Confidential that is not in the Sensitive Compartmented Information or other Special Access Program category.

Combination Lock – A keyless lock that requires the turning of a numbered dial to a preset sequence of numbers for the lock to open. It is usually a three-position, manipulation resistant, dial-type lock, although cipher locks with push buttons are also referred to as combination locks.

Communication Security (COMSEC) – Measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunication, or to mislead unauthorized persons in their interpretation of the results of such possession and study. This includes crypto-security, transmission security, emission security, and physical security of communication security materials and information.

Compartmented Intelligence – National intelligence placed in a DNI-approved control system to ensure handling by specifically identified and access approved individuals.

Compelling Need – A signed determination by a Senior Official of the Intelligence Community, or his/her designee, that the services of an individual, based upon an assessment of risk, are deemed essential to operation or mission accomplishments.

Compelling Need to Apply Safeguarding or Dissemination Controls to Information – When there is a reasonable likelihood that significant or substantial harm will result in particular classified and/or controlled unclassified information if not appropriately protected.

Compromise – When classified information is accessible to persons who do not possess an appropriate security clearance or a need-to-know. An actual or probable compromise of

classified information constitutes a security violation. A compromise of classified information occurs whether the act was intentional or unintentional.

A probable compromise occurs when 1) classified material is recovered outside of controlled area or 2) when the probable controlled area or facility is unattended and not properly secured.

An actual compromise occurs when it is determined that the classified information has been released or disclosed to an unauthorized person(s) or party(ies), and that damage to national security is deemed likely or to have occurred as the result of this unauthorized disclosure.

Comptroller of the Currency (OCC) – The Treasury bureau responsible for chartering, regulating and supervising national banks to ensure a safe, sound, and competitive banking system that supports the citizens, communities and economy of the United States.

Condition – See "Personnel Security – Exception".

CONFIDENTIAL – The classification designation applied to information, the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security that the original classification authority is able to identify or describe. Confidential is also the lowest level of classified information under EO 12958, as amended.

Confidential Source – Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

Configuration Management – The process involving identifying, controlling, accounting for, and auditing all changes made to the baseline system architecture, including hardware, firmware, and software.

Continuous SCIF Operation – Staffing of a SCIF that is manned and operated 24 hours a day, 7 days a week basis.

Contract – Any U.S. Government contract or agreement issued or made by or on behalf of the Secretary of the Treasury, or a Treasury/bureau head.

Contractor Employee – Any non-Federal person employed on a U.S. Government contract.

Contract Security Officer (CSO) – A member of a facility security force and an element of a security post who has the training, equipment, and appropriate certifications to perform a specific security function.

Contracting Officer - A U.S. Government official having written, designated authority to enter into, administer, and/or terminate contracts and make related determinations and findings with respect thereto on behalf of the United States Government.

Contracting Officer's Representative (COR) – An individual designated and authorized by the contracting officer to perform contract administration activities on his/her behalf within the limits of delegated authority for a specific acquisition or contract.

Control – The authority of the agency originating information, or its successor in function, to regulate access to the information.

Controlled Area – A specifically designated area, such as a room, office, building or facility where classified information has been authorized for handling, secure storage, discussion, or processing, and supplemental controls have been established which access is monitored, limited, or controlled.

Controlled Unclassified Information – The exclusive, categorical designation for identifying unclassified information requiring safeguarding and dissemination controls throughout the Executive Branch.

Corroborate – To strengthen, confirm, or make certain the substance of a statement through the use of an independent, but not necessarily authoritative source. For example, the date and place of birth recorded in an official personnel file that could be used to verify the date and place of birth claimed on a Standard Form 86.

Courier – A designated employee or contractor whose on-the-job performance entails routine responsibility for physical transport and secure delivery of classified information between Treasury bureaus and/or to other Federal agencies/departments. All such persons must have the appropriate security clearance at the same level (or higher) of the classified information entrusted to them for safekeeping.

Courier Card – Treasury Department Form (TD F) 15-05.7, designating the bearer as a designated courier for the Department and authorizing him/her to carry classified information up through a specified level, e.g., Secret, Top Secret or TS/SCI.

Counterintelligence – Information gathered and activities conducted to protect against espionage, subversive, terrorist and/or other intelligence activities, sabotage, and assassinations

conducted for, or on behalf of, foreign powers, organizations, or persons. Personnel, physical, document (information), and communications security programs are unrelated to counterintelligence activities and programs unless an association is established through counterintelligence functions.

Counterintelligence Inquiry – Any investigative actions taken to determine the nature and circumstances of incidents subject to counterintelligence purview.

Counterintelligence Support – Counterintelligence activities designed and conducted to identify, exploit, and neutralize real or potential threats of foreign intelligence services and terrorist activities.

Countermeasure – A security device, procedures, or person designed and implemented or trained to mitigate the risk of identified credible threats to a facility.

Credit Check – Information, provided by credit bureaus or other reporting services, pertaining to the credit history of the subject of a personnel security investigation.

Critical-Sensitive – The sensitivity designation for a job (position) having the potential for *exceptionally grave* damage to the national security.

Crypto – A marking or designation identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive information.

Cryptology – The branch of knowledge which treats the principles of cryptography and crypto-analytics and the activities involved in producing signals intelligence (SIGINT) and maintaining communications security (COMSEC).

Custodian – Any person who has possession of, is charged with, or otherwise has been assigned responsibility for the control and accountability of classified information.

Damage Assessment – An analysis of the impact on the national security of the loss or disclosure of classified information to an unauthorized person.

Damage to the National Security – Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Dangerous Weapon – A weapon, device, instrument, material, or substance (animate or inanimate) that is used for or is readily capable of causing death or serious bodily injury, excluding a pocket knife with a blade of less than two-and-a-half inches in length.

Data – Information, regardless of its physical form or characteristics, that includes written documents, automated information systems storage media, maps, charts, paintings, drawings, films, pho0tos, engravings, sketches, working notes, and papers, reproductions thereof by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

Declassification – The authorized change in the status of information from classified to unclassified information.

Declassification Authority – Officials delegated declassification authority in writing by the Secretary of the Treasury or the Department's Senior Agency Official (SAO) responsible for Treasury's information security program.

Declassification Guide – Written instructions issued by a declassification authority describing the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

Decontrol - The lapse of status for information previously designated as Controlled Unclassified Information (including Limited Official Use and Sensitive But Unclassified) from the safeguarding and dissemination control requirements or an authorized action to remove such requirements.

Defensive Travel Briefing – Formal advisories that alert travelers to the potential for harassment, exploitation, provocation, capture, entrapment, terrorism, or criminal activity. These briefings include recommended courses of action to mitigate adverse security and personal consequences and suggest passive and active measures to avoid becoming a target or inadvertent victim.

Degausser – A device that erases magnetically encoded information from recording tapes, data disks, card keys, recording heads, and other magnetized items.

Denial – An adjudicative decision – based on a personnel security investigation, other relevant information, or both – that a candidate for access to sensitive or classified information is ineligible for such access.

Departmental Offices (DO) – The Treasury Offices composed of divisions mostly headed by Assistant Secretaries (or equivalent level), who report to Under Secretaries, and are primarily responsible for policy formulation and overall management of the Treasury Department. These include Domestic Finance, Economic Policy, General Counsel, Information and Technology Management, International Affairs, Management/Chief Financial Officer, Public Affairs, Tax Policy, and Terrorism and Financial Intelligence as well as the Treasurer of the United States.

Derivative Classification – Incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply 1) to the source information or 2) in accordance with security classification guide/guidance, or 3) classified information obtained during a meeting, or 4) similar information obtained via secure fax/phone. The duplication or reproduction of existing classified information is not derivative classification.

Derogatory Information – Issue information that adversely reflects on the person's loyalty, reliability and trustworthiness.

Designated Intelligence Disclosure Official (DIDO) – The heads of IC organizations or those U.S. Government officials who have been designated by the DNI, in writing, as having the authority to approve or deny disclosure or release of uncaveated intelligence information to foreign governments in accordance with applicable disclosure policies and procedures.

Designated Official – The highest-ranking official of the primary agency occupying a Federal facility, or, alternatively, the individual selected by mutual agreement of that agency.

Designation – In an information security context, the determination, made pursuant to EO 13526 that a compelling need to protect a category of information exists, the level of protection required, and the extent of dissemination authorized.

Deterrent – Any physical or psychological device or method that discourages action such as locks or window grilles and the presence of guards or surveillance cameras.

Deviation – See "Personnel Security – Exception".

Disclosure – The communication or physical transfer of classified information to an unauthorized recipient. Showing or revealing classified information, whether orally, in writing or any other medium, without providing the recipient material for retention.

Disseminate or Dissemination – The release or disclosure of information under agency control to any individual, agency, or other entity. Dissemination includes providing an individual, agency or other entity direct access to information without physically releasing the information from agency control.

Document – Any recorded information regardless of its physical form, media, or characteristics, including, without limitation, written or printed matter, tapes, maps, charts, drawings, photos, engravings, sketches, working notes and papers, and reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form.

Downgrading – The determination by a downgrading/declassification authority that information classified and safeguarded at a specific level shall be classified and safeguarded at a lower level.

Dual Citizen – Any person who is simultaneously a citizen of more than one country.

Economic Espionage – Foreign power-sponsored or coordinated collection activity directed at the U.S. Government, U.S. corporations, establishments, or persons involving: (1) the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information, proprietary economic information, or critical technologies, or (2) the unlawful or clandestine targeting or influencing of sensitive economic policy decisions.

Efficiency-of-the-Service – Conduct of an individual expected not to interfere with or prevent effective performance either in the position (applied for or employed in) or by the employing agency of its duties and responsibilities.

Eligibility-for-Access – A favorable adjudication of an appropriate investigation of the subject's background.

Emergency Action Plan (EAP) – A plan developed to prevent loss of national intelligence, classified information, protect personnel, facilities, and communications; and recover operations damaged by terrorist attack, natural disaster or similar events.

Employee – A person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of persons who act for or on behalf of an agency as determined by the appropriate agency head.

Employee Assistance Program (EAP) – A program designed to provide counseling and referral services to employees having personal, alcohol, drug, financial, behavioral, or emotional problems.

Entry-On-Duty (EOD) – The first day that a new employee or contract employee commences employment or reports to his/her duty station for work.

Equity – Information 1) originally classified by or under the control of an agency; 2) in the possession of the receiving agency in the event of transfer of function; or 3) in the possession of a successor agency for an agency that has ceased to exist.

Espionage – Overt, covert, or clandestine activity designed to obtain information relating to the national security with intent or reason to believe that it will be used to the harm of the United States, or to the advantage of a foreign nation.

Event – An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of particular information.

Exception – See "Personnel Security – Exception".

Exempted – Nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification under EO 13526.

Expanded National Agency Check – A personnel security investigation requiring expansion of information developed from the National Agency Check.

Facility – A plant, laboratory, office, college/university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. A business or educational organization may consist of one or more facilities.

Facility Accreditation – An official determination of the physical, procedural and technical security acceptability of a facility and that authorizes its use to protect classified information.

Facility Certification – An official notification to the accreditor of the physical, procedural and technical security acceptability of a facility to protect classified information

Facility Security Clearance (FSC) – An administrative determination that, from a security viewpoint, a (contractor) facility is eligible for access to classified information of a certain category (and all lower categories). The facility security clearance is issued by and under cognizance of the Defense Security Service through the National Industrial Security Program.

Facility Security Committee (FSC) – A body consisting of representatives of the General Services Administration (GSA), the Federal Protective Service (FPS), and each tenant agency occupying a facility protected by the FPS. Among its other duties, the FPS is responsible for reviewing and approving countermeasure recommendations, funding countermeasure applications, and identifying and addressing the facility's security concerns.

Federal Record – All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor

as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the information value of data in them. Library and museum material made or acquired and preserved solely for reference and stocks of publications and processed documents are not included.

Fiduciary – One, such as an agent or director, standing in a special relation of trust, confidence, or responsibility in certain obligations to others, pertaining to, or consisting of money that is not convertible into coin or specie but derives its value from public confidence or government decree.

File Series – File units or documents arranged according to a filing system or kept together because they relate to a specific kind of transaction, take a particular physical form , or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

Financial Crimes Enforcement Network (FinCEN) – The Treasury bureau responsible for supporting law enforcement investigative efforts and fostering interagency and global cooperation against domestic and international financial crimes. FinCEN provides U.S. policy makers with strategic analyses of domestic and worldwide trends and patterns.

Financial Disclosure – A personnel security requirement for clearance processing that requires subjects to provide information regarding their total financial situation, e.g., assets, liabilities and indebtedness.

Financial Management Service (FMS) – The Treasury bureau responsible for receiving and distributing public monies, maintaining government accounts and preparing daily and monthly reports on the status of government finances.

Forced Entry – Entry by an unauthorized individual(s) that leaves evidence of the act.

Foreign Contact – Contact with any person who is not a U.S. citizen or a U.S. national.

Foreign Contact Reporting – The reporting of information concerning instances of official and unofficial contact between U.S. Government employees and non-U.S. citizens whenever 1) illegal or unauthorized access is sought to classified or otherwise sensitive information and technology or 2) circumstances cause the employee to feel concerned he or she might be a target of an actual or attempted exploitation by a foreign entity.

Foreign Government Information (FGI) – Information provided to or produced by, or received by the U.S. Government by a foreign government or governments, an international

organization of governments or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence.

Foreign Intelligence – Information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.

Foreign Intelligence Service (FIS) – The collective term associated with a foreign country's internal security forces and foreign intelligence collection capability. The term is used to refer to all aspects and intelligence disciplines that the service under discussion may possess.

Foreign National – 1) An individual who is not a U.S. citizen or 2) not lawfully authorized permanent resident alien status to reside in the United States.

Foreign Ownership, Control or Influence (FOCI) – A U.S. company is considered under foreign ownership, control or influence whenever a foreign interest has the power, direct or indirect, whether or not exercised and whether or not exercisable through ownership of the U.S. company's security, by contractual arrangement or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information and/or special nuclear material or may affect adversely the performance of classified contracts.

High Risk Positions – Positions that have the potential for exceptionally serious impact on the "efficiency of the service" involving duties especially critical to the agency or a program mission with broad scope of policy or program authority.

Hyper Text Markup Language – The authorizing language used to create document on the World Wide Web.

Hypertext Statement - A portion of text linked to another document, or another section of a document. It is usually in a different color than the rest of the text and if you place your cursor over it, the cursor will change showing that it is a hyperlink.

Illegal Drug Use – The use of drugs, possession or distribution of which is unlawful under the Controlled Substances Act. Such term does not include the use of a drug taken under the supervision of a licensed health care professional, other uses authorized by the Controlled Substances Act or other provisions of law.

Immediate Family Member – For purposes of personnel security vetting, immediate family members include the spouse, parents, siblings, children, stepchildren and cohabitant of subject or applicant.

Incident – Any event affecting the safety, security, or protection of property, a facility, or occupant (or visitor) that requires a response, investigation, or other follow-up-. Events that, at the time of occurrence, cannot be determined to be an actual violation of law, but which are of such significance as to warrant preliminary inquiry and subsequent reporting. Examples include drug use and distribution, alcohol abuse, the discovery or possession of contraband articles in security areas, and unauthorized access to classified data.

Indoctrination – Formal instruction to an individual approved for access to Sensitive Compartmented Information or Special Access Programs regarding program-unique and program-specific security requirements and responsibilities.

Industrial Security - That segment of security concerned with protecting classified information released to and in the possession of contractors. This term describes the program under which the U.S. Government engages in a contract (unclassified or classified) that has security policies and responsibilities for safeguarding the information, information systems, assets, or facilities, which are imposed on the contractor, and in which the U.S. Government provides guidance to and conducts oversight of contractor implementation of those policies. See National Industrial Security Program (NISP).

Immigrant alien – Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

Information – Any knowledge that can be communicated or documentary material, regardless of its physical form, media, or characteristics, which is owned by, produced by or for, or is under the control of the U.S. Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information Assurance – Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Security – The program established by Executive Order for the classification, declassification, downgrading and safeguarding of classified information. This also includes protection of sensitive but unclassified (non-national security) information.

Information system (IS) – Is any combination of information technology and people's activities using that technology to support operations, management, and decision-making.

Infraction – A security incident involving a deviation from governing security regulations that does not result in an unauthorized disclosure or compromise of classified information nor otherwise constitutes a security violation.

Insider Threat – The ability of a trusted insider to bypass or defeat security safeguards or otherwise adversely affect the national security.

Inspector General (OIG) – The OIG conducts independent audits, investigations and reviews to help the Treasury Department accomplish its mission; improve its programs and operations; promote economy, efficiency and effectiveness; and prevent and detect fraud and abuse.

Integral File Block – A distinct component of a file series that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time such as a presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

Integrity – The state that exists when information is unchanged from its source and has been accidentally or intentionally modified, altered, or destroyed.

Intelligence Activities – A generic term used to encompass any or all of the efforts and endeavors undertaken by intelligence organizations, including activities pursuant to collection, analysis, production, dissemination, and covert or clandestine activities. When used in the context of EO 12333, as amended, or a successor order it means all activities that agencies within the Intelligence Community are authorized to conduct.

Intelligence Community – A generic term defined in EO 12333 which refers to the following agencies or organizations: the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the Bureau of Intelligence and Research of the Department of State; the intelligence elements of the Army, Navy, Air Force and Marine Corps, the FBI, the Department of the Treasury's Office of Intelligence and Analysis, and the Department of Energy.

Intelligence Sources and Methods – (1) Sources: Persons, images, signals, documents, databases, and communications media capable of providing intelligence information through collection and analysis programs; and (2) Methods: Information collection and analysis strategies, tactics, operations and technologies employed to produce intelligence products. If intelligence sources or methods are disclosed without authorization, their effectiveness may be substantially negated or impaired.

Interim Security Clearance – A security clearance based on the completion of minimum investigative requirements that is granted on a temporary basis pending the completion of full investigative requirements, including receipt and adjudication of the individual's completed background investigation.

Internal Revenue Service (IRS) – The largest Treasury bureau, the IRS is responsible for determining, assessing, and collecting internal revenue in the United States.

Internal Vulnerability – The inside threat posed by an individual, with access to classified national intelligence, including Sensitive Compartmented Information, who may betray his or her trust.

Intrusion Detection System (IDS) – A technical security system designed to detect an attempted or actual unauthorized entry into a secure facility or information systems and alert responders.

Investigation – A comprehensive examination of facts or other pertinent information.

Issue Case – A case containing any issue information, even if fully mitigated.

Joint Personnel Adjudication System (JPAS) – The centralized Defense Department database of standardized processes; virtually consolidates the Defense Central Adjudication Facilities by offering real time information concerning clearances, access, and investigative statuses to authorized security personnel and other interfacing organizations.

Key – (1) An object that carries the mechanical code configuration that unlocks a locking mechanism. (2) A system for transforming a cryptogram or cipher to plain text.

Law Enforcement Officer (LEO) – An officer, agent, or employee of the United States, a state or tribal government, or a political subdivision thereof, authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of law.

Lawful Permanent Resident (LPR) – A non-U.S. citizen who has been lawfully admitted into the United States and accorded the privilege of residing permanently in the United States as an immigrant in accordance with the immigration laws, such status not having changed.

Lead – Single investigative element of a case requiring action. Leads include reference interviews, record checks, subject interviews, local agency checks, and national agency checks.

Letter or Statement of Compelling Need – A written statement by a program manager or designee that the services of an individual with access eligibility issues, e.g., lacking U.S. citizenship or having foreign national family members, are essential to mission accomplishment.

Limited Access Authorization (LAA) – Authorized access to classified information where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed and for which a cleared or clearable U.S. citizen is not available and 1) access is limited to classified information relating to a specific project or product, 2) the appropriate foreign disclosure authority determines that access to classified information is consistent with authority to release the information to the individual's country of origin. Further limitations are: no physical custody of classified information, not granted to perform routine administrative or other support duties, individual will not be designated as a courier or escort for classified information or permitted uncontrolled access to areas where classified information is stored or discussed (classified information will be maintained in a location under continuous control and supervision of appropriately cleared U.S. citizen), a Single-Scope Background Investigation is completed covering the prior 10 years of the subject's live, and the individual agrees to a counter-intelligence polygraph before being granted access.

Limited Background Investigation (LBI) – A suitability or security investigation consisting of both record checks and credit checks and a NAC, and interviews with the candidate and selected sources covering the last 3 years of an individual's life.

Local Agency Check/Local Law Enforcement Check – An inquiry consisting of a review of criminal history information maintained by state and local authorities.

Local Entities – A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or intestate government entity, or agency or instrumentality of a local government; and a rural community, unincorporated town or village, or other public entity as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101(11)).

Low Risk Position – Positions involving duties that have the potential for limited impact upon the agency mission based upon their limited program responsibilities that affect the "efficiency of the service".

Mandatory Declassification Review – Review for declassification of classified information in response to a request for declassification that meets the requirements of Executive Order 13526.

Material – Any product or substance on or in which information is embodied.

Memorandum of Agreement (MOA) – A written agreement among relevant parties that specifies roles, responsibilities, terms and conditions for each party to reach a common goal.

Metadata - Metadata is a concept that applies mainly to electronically archived data and is used to describe the a) definition, b) structure and c) administration of data files with all contents in

context to ease the use of the captured and archived data for further use. Web pages often include metadata in the form of "meta" tags. Description and keywords "meta" tags are commonly used to describe the Web page's content. Most search engines use this data when adding pages to their search index. Metadata is loosely defined as data about data and the strength of this definition is in recognizing that metadata is data. Metadata can be stored and managed in a database, often called a registry or repository. However, it is impossible to identify metadata just by looking at it.

Minimum Background Investigation (MBI) – A personnel suitability/security investigation consisting of a national agency check and inquiry (NACI), personal interview, credit search, written inquiries and record searches covering specific areas of a subject's background in the past five (5) years.

Mission-Essential Functions – Continuing functions that must be performed without unacceptable disruption to achieve Treasury's critical missions.

Mitigating Information – Personnel security information that tends to explain or refute factors that could otherwise support denial, revocation, or the granting of access only with an exception.

Moderate Risk Position – Positions involving duties having the potential for moderate to serious impact on an agency or a program mission with significant program responsibilities and delivery of customer services to the public.

Multiple Sources – Two or more source documents, classification guides, or a combination of both used as the basis for classifying particular information.

National - A person owing permanent allegiance to a state. The term "national of the United States" means (a) a citizen of the United States, or (b) a person who, though not a citizen of the United States, owes permanent allegiance to the United States.

National Agency Check (NAC) – A personnel suitability/security investigation consisting of a records review of certain national agencies including a technical fingerprint and name search of the files of the Federal Bureau of Investigation.

National Agency Check plus Written Inquiries (NACI) – A personnel suitability/security investigation conducted by the Office of Personnel Management combining a NAC with written inquiries to law enforcement agencies, former employers and supervisors, references, and schools.

National Agency Check with Local Agency Checks and Credit Check (NACLC) – The investigation to be used in reinvestigating employees/contractors who have the need for Secret and Confidential security clearances.

National Declassification Center (NDC) – The entity established within the National Archives and Records Administration to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training for declassification of records determined to have permanent historical value.

National Industrial Security Program (NISP) – The single, integrated, cohesive security program established by Executive Order 12829 to protect classified information provided to or developed by contractors and applicable to all Executive Branch departments and agencies.

National Intelligence – All intelligence, regardless of the source from which derived and including information gathered within or outside the U.S., that 1) pertains, as determined consistent with any guidance issued by the President, to more than one U.S. Government agency; and 2) that involves: threats to the U.S., its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on U.S. national or homeland security.

National Interest – The well-being and security of the United States, this applies to the furtherance of the nation's foreign policy objectives and overseas interests; protection of the nation from internal subversion, sabotage, espionage, and other illegal acts as well as from foreign aggression; promotion of domestic well-being and the economic and productive strength of the nation; and fulfillment of the public trust through the proper and lawful conduct of the U.S. Government's business.

National Security – The national defense or foreign relations of the United States and includes, with a Treasury context, U.S. economic vitality, global competitiveness, market sensitivity and tracking terrorist assets/financial crimes.

National Security Clearance – Certification issued by a designated personnel security official or designee that a person may access classified information on a need-to-know basis.

National Security Emergency – Any occurrence including, but not limited to, natural disaster, attack, technological failure, civil unrest, or other disruptive condition that would seriously degrade or threaten the national security of the U.S.

National Security Information (NSI) – Any information that has been determined, pursuant to Executive Order 13526, or any predecessor order, to require protection against unauthorized disclosure and this is so designated; also known as "collateral" information.

National Security Positions – Those positions under EO 10450 involving activities of the Government concerned with protecting the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities,

foreign relations, and related activities concerning the preservation of the military strength of the United States; and positions that require regular use of, or access to, classified information.

Need-for-Access – A determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

Need-to-Know – The determination by an authorized holder of classified information that access to that particular information is required by another appropriately cleared individual to perform official duties.

Newly Discovered Records – Records that were inadvertently not reviewed prior to the effective date of automatic declassification because the agency declassification authority was unaware of their existence.

Non-Critical Sensitive – Sensitivity designation of a position that has the potential for limited damage to the national security and equating to a low risk position designation.

Non-Disclosure Agreement (NDA) – An officially authorized contract between an individual and the U.S. Government signed by an individual as a condition of access to classified information and specifying the security requirements for the access and details the penalties for noncompliance.

Non-Discussion Areas – A defined area within a SCIF where classified discussions are not authorized.

Non-Sensitive Position – A position that does not require access to classified information and that has low risk to the national security and public trust.

Occupant – An employee or contract employee permanently or regularly assigned to a facility. This may also include the employees of non-Federal tenants of a facility. The FSC establishes thresholds for determining who qualifies for "occupant" status.

Offense – A violation of Federal, state, or local criminal law or regulation for which a violator could be subject to prosecution.

Office of Management and Budget (OBM) – The U.S. Government element designated by Executive Order 13381 that is responsible for improving the process by which the government determines eligibility for access to classified information.

Office of Personnel Management (OPM) – The U.S. Government element responsible for day-to-day supervision and monitoring of security clearance investigations and for tracking the results of individual agency-performed adjudications.

Office of Thrift Supervision (OTS) – This Treasury bureau is the primary regulator of Federal and many state-chartered thrift institutions, which includes savings banks and savings and loan associations.

Open Storage – The storage of classified information on shelves or in locked or unlocked non-approved containers when authorized personnel do not occupy the facility. In all instances, "Open Storage" must be specifically approved by Treasury or bureau headquarters security officials to store classified information and is limited to the Secret level.

Operations Security (OPSEC) - A systematic process intended to deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Original Classification – The initial determination information requires, in the interest of the national security, protection against unauthorized disclosure.

Original Classification Authority (OCA) – An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance. Within Treasury, OCAs are designated by the Secretary (at the Top Secret, Secret, or Confidential levels) or by the Department's Senior Agency Official (at the Secret or Confidential levels).

Oversight Reviews – Formal (or informal) examinations of implementation of national and Treasury/bureau security policies, practices and procedures including staffing.

Page Metadata – The HTML code that is built into a web document.

Paragraph or Portion Markings – Required markings on classified documents to indicate the specific level of classification applicable to each paragraph or portion of a document shown in parenthetical form as follows: (TS) for TOP SECRET, (S) for SECRET, (C) for CONFIDENTIAL and (U) for UNCLASSIFIED.

Pass/Fail – A declassification technique that regards information at the full document or folder level. Any exemptible portion of a document or folder might result in exemption (failure) of the entire documents or folders. Documents or folders that contain no exemptible information are

passed and therefore declassified. Documents within exempt folders are exempt from automatic declassification. Declassified documents may be subject to FOIA exemptions other than the security exemption ((b) (1)), and the requirements placed by legal authorities governing Presidential records and materials.

Periodic Re-investigation (PR) – A re-investigation of an employee currently holding a security clearance or a public trust position. A periodic reinvestigation is required every 5 years for a Top Secret clearance, 10 years for a Secret clearance, or 15 years for a Confidential clearance. Positions designated critical-sensitive, high risk, and law enforcement or public trust positions that are designated moderate risk, are subject to a periodic reinvestigation every five years.

Permanently Historically Valuable Records – Presidential papers/records and the records of an agency that the Archivist of the United States has determined should be maintained permanently in accordance with 44 U.S.C.

Permanent Resident Alien – Any alien lawfully admitted into the U.S. under an immigration visa for permanent residence. Also referred to as a "lawful permanent resident".

Personal Financial Statement – Form used as part of a personnel security investigation to provide a summary of a person's total monthly income, debt payments, expenses, and the net remainder of income.

Personally Identifiable Information (PII) - Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Personnel Background Investigation – An investigation conducted by written or telephone inquiries or through personal contacts to determine the suitability, eligibility, or qualifications of individuals for Federal employment, for work on Federal contracts, or for access to classified information or restricted areas.

Personnel Security – The segment of security that concerns the trustworthiness and integrity of Federal employees and others associated with the U.S. Government. It is also the process in the U.S. Government for complying with national security interest requirements under EO 10450 or with other similar authority.

Personnel Security Clearance (PCL). An administrative determination that an individual is eligible, from a security viewpoint, for access to classified information at the same or lower category as the level of the personnel clearance being granted.

Personnel Security Exception – An adjudicative decision to grant or continue access eligibility despite a failure to meet all adjudicative or investigative standards. For purposes of reciprocity, the presence of an exception permits the gaining organization or program to review the case before assuming security sponsorship and to accept or decline sponsorship based on that review. When accepting sponsorship, the gaining organization or program will ensure that the exception remains a matter of record. There are three types of exceptions: conditions, deviations, and waivers.

1) Conditions: Access eligibility granted or continued with the provisions that additional security measures shall be required. Such measures include, but are not limited to, additional security monitoring, access restrictions, submission of periodic financial statements, and attendance at counseling sessions.

2) Deviations: Access eligibility granted or continued despite a significant gap in coverage or scope in the investigation or an out-of-date investigation. "Significant gap" for this purpose means either complete lack of coverage for a period of six months or longer within the most recent five years investigated or the lack of an FBI name check or technical check or the lack of one or more relevant investigative components (e.g., employment checks, financial review, or a subject interview) in its entirety.

3) Waivers: Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. Waivers by appropriate authority may only be approved when the benefit of access clearly outweighs any security concern raised by the shortcoming. A waiver may require prescribed limitations on access such as additional security monitoring. See "Personnel Security – Issue Information".

Personnel Security Interview – An interview conducted with an applicant for or h older of a security clearance to discuss areas of security relevance. The term is also used to describe interviews with references in personnel security investigations.

Personnel Security Issue Information – Any information that could adversely affect a person's eligibility for classified information. There are two types of issue information:

1) Minor Issue Information: Information that meets a threshold of concern set out in "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," but for which adjudication determines that adequate mitigation, as provided by the Guidelines, exists. Minor issue information does not provide the basis for a waiver or condition.

2) Substantial Issue Information: Any information, or aggregate of information, that raises a significant question about the prudence of granting access eligibility. Substantial issue

information constitutes the basis for granting access eligibility with waiver or condition, or for denying or revoking access eligibility.

Personnel Security Questionnaire (PSQ) – Security forms, whether paper or electronic, that are completed by a subject as part of a personnel security investigation; Standard Forms (SF) 85, 85P and 86.

Phased Periodic Reinvestigation – A periodic reinvestigation which may exclude references and neighborhood check requirements when no information of security concern is developed through the other reinvestigation requirements.

Physical Security – The segment of security concerning protective requirements and means for safeguarding Treasury personnel, property, facilities and information.

Portable Electronic Devices (PEDs) – Electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples include, but are not limited to, pagers, laptops, cellular phones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders.

Position Sensitivity – Designation based on an assessment of the degree of damage that an individual, by virtue of the occupancy of a position, could have an effect on the national security.

Preliminary Inquiries – Activities conducted for the purpose of assessing whether or not an incident or other matter of security concern involving classified or sensitive information is a CI investigative matter.

Presidential Historical Materials and Records – The papers or records of the former Presidents under the legal control of the Archivist of the United States.

Prime Contract - A contract let by a Government Contracting Activity (GCA) to a contractor.

Private Sector - Persons outside Government who are critically involved in ensuring that public and private preparedness and response efforts are integrated, including: 1) corporate owners and operators determined by the Secretary of Homeland Security to be part of the Critical Infrastructure/Key Resources (CI/KR); 2) subject matter experts selected to assist the Federal or State CI/KR; 3) personnel serving in specific leadership positions of CI/KR coordination, operations and oversight; 4) employees of corporate entities relating to the protection of CI/KR; or 5) other persons not otherwise eligible for the granting of a personnel security clearance pursuant to Executive Order 12829, as amended, who are determined by the Secretary of Homeland Security to require a personnel security clearance.

Prohibited Item – An item, legal or illegal, restricted from entry into a facility by Federal, state, or local law, regulation, court order, rule or FSC policy.

Proprietary Information – All forms of information, including financial, business, scientific, technical, economic and engineering information, regardless of its form, under the control of an owner, provided the owner has taken reasonable measures to keep the information from public disclosure. Reasonable measures include marking and/or notifying the recipient of the disclosure restrictions.

Public Law (PL) – A law affecting the public at large. It is a theory of law governing the relationship between individuals (citizens, companies) and the state.

Public Trust Positions – All positions not designated as national security positions shall be designated as high, moderate, or low risk as determined by the position's potential for adverse impact to the "efficiency of the service". Public trust positions are those positions designated moderate and high risk.

Questionnaire for National Security Positions – The Standard Form 86 developed by the Office of Personnel Management for background investigations and reinvestigations. Completed by the applicant, the SF86 provides details on various aspects of the individual's personal and professional background; also known as the "PSQ".

Reciprocity – Recognition and acceptance, without further processing of 1) security background investigations and clearance eligibility determinations; 2) accreditations of information systems; and 3) facility accreditations.

Records – Official records of an agency and Presidential papers/records including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate or grant.

Records Management – Planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the U.S. Government and effective and economical management of agency operations.

Redaction – The removal of exempted information from copies of a document.

Reference – A person, other than the subject of a background investigation, identified as having knowledge of the subject. References are characterized by source and by type. There are two sources: 1) Listed (meaning the subject of the investigation identified the reference on the SF 86

and 2) Developed (meaning an investigator, in the course of pursuing leads, identified the reference as someone knowledgeable of the subject). There are six types:

1) Education (a faculty member or school administrator at a school attended by the subject who had knowledge of the subject when a student).

2) Employment/Supervisor (a person with management responsibilities for the subject).

3) Co-worker (a colleague with knowledge of the subject's on-the-job behavior).

4) Friend/Associate (a person knowing the subject socially preferably away from both work and home).

5) Knowledgeable Person (a person who knows the subject in some other context, for example, a banker or attorney or real estate agent who conducts business on behalf of the subject; or a clerk in a store where the subject shops frequently). A specific reference can be categorized as more than one type, for example, someone who is both an office mate and fellow member of a softball team may be both a co-worker reference and a friend/associate reference.

Referral - Information in an agency's records that was originated by or is of interest to another agency and sent to that agency for a determination of its classified status.

Regrade – To raise or lower the classification assigned to an item of information.

Reinstatement – A process whereby an individual whose access authorization has been terminated or revoked I s permitted to again have classified information.

Release – Providing classified information in writing or any other medium for retention. See "Disclosure".

Remote Archives Capture (RAC) Project – A collaborative program to facilitate the declassification review of classified records in the Presidential Libraries in accordance with section 3.3, Executive Order 13526. In this project, classified Presidential records at various Presidential Libraries are scanned and brought to the Washington, DC, metropolitan area in electronic form for review by equity-holding agencies.

Restricted Area – A room, office, building, or facility to which access is strictly and tightly controlled. Admittance to a restricted area is limited to personnel assigned to the area or persons who have been authorized access to the area. Personnel assigned to the area must escort visitors to a restricted area and un-cleared personnel and all classified and sensitive information must be protected from observation, disclosure, or removal. The servicing security officer is authorized to designate restricted areas after appropriate security measures are in place.

Restricted Portal – A protected community of interest or similar compartmented area housed within an information system and to which access is controlled by a host agency different from the agency that controls the information system.

Revocation – An adjudicative decision to permanently withdraw an individual's clearance based on a personnel security investigation, other relevant information, or both, that a cleared person is no longer eligible for access to classified information.

Risk – The probability of loss from an attack, or adverse incident. It is a function of threat (adversaries' capabilities, intentions and opportunities) and vulnerability (the inherent susceptibility to attack). Risk may be quantified and expressed in terms such as cost in loss of life, dollars, resources, programmatic impact, etc.

Risk Analysis – An analysis of system assets and vulnerabilities to establish an expected loss from certain events based upon estimated probabilities of the occurrence of these events.

Risk Assessment – The process of evaluating security risks based on analyses of threats, vulnerabilities, and probable adverse consequences to a facility, system, or operation.

Risk Designation – Position designation based on an assessment of the degree of adverse impact that an individual, by virtue of the occupancy of the position, could effect on an agency or program mission, or on the overall "'efficiency of the service".

Risk Management – The process of selecting and implementing security countermeasures to accept or mitigate the risk of a known or suspected threat to an acceptable level based on cost and effectiveness. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

Sabotage – The willful destruction or injury of, or defective production of information, material or property of the government.

Safe – A GSA-approved security container equipped with a built-in (mounted), dial-type, changeable combination lock, specifically designed for the classified information. A safe may also be used for protecting money and other highly negotiable materials or assets.

Safeguarding or Safeguards– Physical, procedural or electronic measures and controls prescribed to ensure classified and controlled unclassified information is not accessed inadvertently or improperly.

Scattered Castles – The Intelligence Community security clearance repository and the Director of National Intelligence's authoritative source for clearance and access information for all IC, military services, Defense Department civilians, and contractor personnel.

Scheduled Records - All records that fall under a National Archives and Records Administration approved records control schedule.

Scope – The time period to be covered and the sources of information to be contacted during the prescribed course of a personnel security investigation.

Screener – An individual (LEO or contract CSO) performing a screening function as a security post.

Screening Event – The presentation, review, decision, and disposition related to an object being introduced into a facility, whether in plain view, concealed on a person, or in a container.

SECRET – The classification level applied only to information the unauthorized disclosure of which reasonably could be expected to cause *serious* damage to the national security that the original classification authority is able to identify or describe.

Secure Room – A room that offers the same or greater protection than a GSA-approved security container authorized for the storage of classified material, through the use of a combination of guards, detectors/alarms, and/or locking devices.

Secure Terminal Equipment (STE) - The U.S. Government's current (as of 2008), encrypted telephone communications system for wired or "landline" communications.

Secure Working Area – An area accredited for handling, discussing and/or processing of classified information to include SCI, but NOT for the storage of classified information.

Security Assurance – An administrative determination based upon the results of personnel security processing that establishes that no reason exists on security grounds to preclude the association of a non-employee with the Department. Access to classified information is not the basis upon which to litigate such determination.

Security Classification Guide (SCG) - a documentary form of guidance, issued by an original classification authority, providing the user with instructions on what types of information may be classified and the level/duration thereof. See Treasury's consolidated classification guide dated March 23, 2008.

Security Clearance – An administrative authorization for access to national security information, up to a stated classification level (Top Secret, Secret, or Confidential) and also referred to as a "clearance".

Security Countermeasures – Actions, devices, procedures, and/or techniques to reduce security risks.

Security Force System – A countermeasure system comprising a security post or posts and associated personnel, equipment, and other elements dedicated to performing security functions that reduce physical security vulnerabilities for an asset or collection of assets and which is the main integrator of all countermeasure systems.

Security Hours – Hours during which a facility is not normally open for business or public access and during which more stringent access controls apply.

Security Incident – An act that constitutes a threat to a security program or is a deviation from existing governing security regulations. Security incidents may be portrayed as security infractions or security violations.

Security-In-Depth – A determination by the agency head (or designee) that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion detection system, random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during non-working hours.

Security Infraction – Any knowing, willful, or negligent action contrary to the requirements of EO 13526 or its implementing directives that does not constitute a security "violation".

Security Post – A countermeasure consisting of one (or more) CSO(s) plus other elements, the purpose of which is to perform a specific security function for the period the countermeasure is active.

Security Screening – An electronic, visual, or manual inspection or search of persons, vehicles, packages, and containers for the purpose of detecting the possession or attempted introduction of illegal, prohibited or other dangerous items.

Security Specialist – A security specialist within the GS-080 series whose primary duties include analytical, planning, advisory, operational, or evaluative work having as its principal purpose the development and implementation of policies, procedures, standards, training, and

methods for identifying and protecting personnel, property, facilities, information, operations, or material from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss. Security specialists also provide specialized program guidance/support, and conduct security surveys, compliance reviews, inquiries, and follow-up action with respect to reported security violations/infractions.

Security Station – A space comprised of an arrangement of multiple security posts to provide an integrated security process at a specific location.

Security/Suitability Investigations Index – The Office of Personnel Management database for personnel security investigations.

Security Survey – A fundamental evaluation and analysis of security-related devices, equipment, services, and procedures in use in a given location, including recommendations for security improvements. The three basic elements examined in a security survey are criticality, vulnerability, and probability. A security survey is a form of risk analysis.

Security System – A term applied to the totality of a facility's security equipment and related procedures, i.e., locks, security containers, guards, access controls, detectors/alarms, etc.

Security Violation – Any knowing, willful, or negligent action 1) that could reasonably be expected to result in an unauthorized disclosure of classified information; 2) to classify or continue the classification of information contrary to the requirements of EO 13526 or its implementing directives; or 3) to create or continue a special access program contrary to this EO.

Self-Assessment/Inspection – The internal review and evaluation of individual agency or component activities and the agency as a whole with respect to implementation of the information security program established by EO 13526 and it's implementing directives.

Senior Agency Official (SAO) – The official designated by the agency head under EO 13526 to direct and administer the agency's security program, under which information is classified, safeguarded/handled, and declassified.

Senior Official of the Intelligence Community (SOIC) – The head of an agency, organization, bureau, office, intelligence element or activities within the IC, as defined in Section 3 of the National Security Act of 1947, as amended and EO 12333; within the Department of the Treasury, the Assistant Secretary of the Office of Intelligence and Analysis.

Sensitive But Unclassified Information (SBU) – Unclassified information Treasury, bureaus, or another authority has determined to require protection from unauthorized or unwarranted public disclosure.

Sensitive Compartmented Information (SCI) – Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director of Central Intelligence and requiring limited access and control on its dissemination; also known as "codeword" information.

Sensitive Compartmented Information Facility (SCIF) – An accredited area, room, group or rooms, buildings, or installation certified and accredited as meeting Director of National Intelligence security standards for the processing, storage and/or discussion of SCI.

Sensitive Position – Any position within Treasury, the occupant of which could bring about, by virtue of the nature of the position and access to classified information, a materially adverse effect on the national security, the mission of the Department, or the "efficiency of the service". All sensitive positions are designated as either special sensitive, critical-sensitive, or non-critical sensitive.

Single Linear Text String – A single line of text versus multiple lines of text.

Single Scope Background Investigation (SSBI) – A personnel suitability/security investigation consisting of personal interviews and record searches covering the most recent ten (10) years of an individual's life or back to their 18th birthday, in any case not beyond the 16th birthday. This investigation replaces the special background investigation and is required for those positions considered special sensitive and those critical sensitive positions requiring Top Secret clearance.

Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR) – A periodic personnel security reinvestigation for Top Secret clearances and/or critical sensitive or special sensitive positions, initiated at any time following completion of, but not later than five years, from the date of the previous investigation or reinvestigation.

Sound Masking System – An electronic system used to create background noise to mask conversations and counter audio-surveillance threats.

Source Document -- An existing document containing classified information that is incorporated, paraphrased, restated or generated in new form into a new document.

Special Access Program – A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Special Activities – Activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the U.S. Government is not apparent or

acknowledged publicly, and functions in support of such activities, but which are not intended to influence U.S. political processes, public opinion, policies, or media and do not include diplomatic activities, the collection and production of intelligence, or related support functions.

Special Inspector General for the Troubled Asset Recovery Program (SIGTARP) - The IG component established to oversee the program established for stabilizing the U.S. financial system and preventing a systemic collapse.

Special Investigative Inquiry (SII) – A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination.

Special Security Officer (SSO) – An individual appointed in writing by a cognizant security authority who is responsible for all aspects of SCI security at a U.S. Government facility.

Special-Sensitive – Sensitivity designation of a position that has the potential for *inestimable* damage to the national security.

Sponsoring Agency – An agency that recommends access to or possession of classified information by State, Local, Tribal and Private Sector (SLTPS) personnel.

Staff-like Access – Unescorted access to Treasury-owned or controlled facilities, information systems, security items and products, and/or to areas storing/processing sensitive but unclassified information, as determined by Treasury/bureau officials.

State – Any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guan, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States, as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101(15)).

State, Local, and Tribal Personnel – Governors, mayors, tribal leaders, and other elected or appointed officials of a State, local government or tribe; State, local, and tribal law enforcement personnel and firefighters; public health, radiological health, and medical professionals of a State, local government, or tribe; and regional, State, local, and tribal emergency management agency personnel, including State Adjutants General and other appropriate public safety personnel and those personnel providing support to a Federal CI/KR mission.

Subcontract - Any mutually binding agreement entered into by a contractor to furnish supplies of services for performance of a prime contract.

Subcontractor - A supplier, distributor, vendor or firm that furnishes supplies or services to or for a prime contractor or another subcontractor. A subcontractor is considered a prime contractor in relation to each of its subcontractors.

Subversion – A systematic attempt to overthrow or undermine a government or political system by persons working secretly from within.

Suitability Determination – Suitability refers to identifiable character traits and past conduct, which are sufficient to determine whether an individual is likely or unlikely to be able to carry out the duties of the job with appropriate efficiency and effectiveness. It also refers to statutory or regulatory bars, which prevent the lawful employment of the individual into the position.

Surreptitious Entry – The unauthorized entry into a facility or security container in a manner in which evidence of such entry is not discernible under normal circumstances.

Surveillance – Observation or inspection of persons or premises for security purposes through alarm systems, closed circuit television (CCTV), or other monitoring methods.

Systematic Declassification Review – The review for declassification of classified information contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with 44 U.S.C. 2107.

Tab – A narrow paper sleeve placed around a document or group of documents in such a way that it would be readily visible.

Tactical SCIF – An area, room, group of rooms, building, or installation accredited by SCI-level processing, storage and discussion, that is used for operational exigencies (actual or simulated) for a specified period of time not exceeding one year.

Tear Line – The place in an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the need-to-know, need-to-release, and write-to-release principles and foreign disclosure guidelines of the information below the tear line.

Technical Security – The employment of specialized equipment and methods used to (1) gather information in support of counterintelligence inquiries, operations, and other activities as required, or (2) detect the presence of activities subject to counterintelligence purview.

Technical Surveillance Countermeasures (TSCM) – Employment of services, equipment, and techniques designed to locate, identify, and neutralize the effectiveness of technical surveillance activities; physical, electronic, and visual techniques used to detect and counter technical surveillance devices, technical security hazards, and related physical security deficiencies.

Technical Surveillance Countermeasures Inspection – A government-sponsored comprehensive physical and electronic examination of an area by trained and specially equipped security personnel to detect or counter technical surveillance penetrations or hazards.

Technical Threat Analysis – A continual process of compiling and examining all available information concerning potential technical surveillance activities by intelligence groups which could target personnel, information, operations, and resources.

Telecommunication – The preparation, transmission or communication of information by electronic means.

TEMPEST – An unclassified term that refers to the investigation and study of compromising emanations.

Temporary Access Eligibility – Temporary eligibility for access that is based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

Temporary Secure Working Area (TSWA) - As temporarily accredited facility that is used no more than 40 hours monthly for the handling, discussion, and/or processing of SCI, but where SCI should not be stored, with sufficient justification, the CSA may approve longer periods of usage and storage of SCI for no longer than 6 months.

Termination Security Briefing – A security briefing to remind individuals of their continued security responsibilities when their access authorization has been revoked, terminated, or suspended.

Terrorism – The calculated and illegal use of violence or threat of violence to inculcate fear, intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological in nature.

Text Translator – Translation of text into different (foreign) languages.

Threat – The intention and capability of an adversary to undertake actions that would be detrimental to the interests of the United States.

Threat Analysis – Actions taken to acquire, assemble, and analyze information, which confirms or refutes the existence of known or potential danger to Department employees, information,

TOP SECRET – The designation applied to classified information, the unauthorized disclosure of which reasonably could be expected to *cause exceptionally grave damage* to the national security.

Transferred Records – Federal records approved by the National Archives and Records Administration for disposal, either immediately or after a specified retention period; also called disposable records.

Transportation Security Administration (TSA) – The Federal agency responsible for protecting the Nation's transportation systems to ensure freedom of movement for people and commerce.

Travel (Official) – Travel performed at the direction of the U.S. Government.

Travel (Unofficial) – Travel undertaken by an individual without official fiscal or other obligations on behalf of the U.S. Government.

Treasury Inspector General for Tax Administration (TIGTA) – The TIGTA provides leadership and coordination and recommends policy for activities designed to promote economy, efficiency, and effectiveness in the administration of the internal revenue laws. TIGTA also recommends policies to prevent and detect fraud and abuse in the programs and operations of the Internal Revenue Service and related entities.

Treasury Personnel – Any Federal employee, subcontractor, contractor, detailee, consultant, or other individual employed by, assigned to, or otherwise associated with Treasury programs or facilities and its constituent bureaus.

Tribe – any Indian or Alaska Native tribe, band, nation, pueblo, village or community that the Secretary of the Interior acknowledges to exist as an "Indian tribe" as defined in the Federally Recognized Tribe List Act of 1994 (25 U.S.C. 479a (2)).

Unauthorized Disclosure – A communication or physical transfer of classified information to an unauthorized recipient.

Underwriters' Laboratories, Inc. (UL) – A nonprofit, national testing laboratory that tests and certifies various categories of equipment and electrical devices for safety and reliability.

United States – In a geographic sense, any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the

Commonwealth of the Northern Mariana Islands, any possession of the United States and any waters within the territorial jurisdiction of the United States.

United States Citizen (Native Born) – An individual born in the United States of America and including the District of Columbia, Puerto Rico, Guam, American Samoa, U.S. holdings in the Mariana Islands, the U.S. Virgin Islands, the Federated States of Micronesia, the Republic of the Marshall Islands, or the Panama Canal Zone (if the father or mother (or both) was or is a citizen of the United States).

United States Mint – The Treasury bureau responsible for designing and manufacturing domestic, bullion and foreign coins as well as commemorative medals and other numismatic items. The Mint also distributes U.S. coins to the Federal Reserve banks and maintains physical custody and protection of the nation's silver and gold assets.

Unscheduled Records – Federal records whose final disposition has not been approved by the National Archives and Records Administration.

User or End User- A person or processer authorized to access an information system.

Vault – An area approved by the agency head (or designee) which is designed and constructed of masonry units or steel lined construction to provide protection against forced entry and equipped with a GSA-approved vault door and lock.

Verify – To accept a statement as true based upon confirmation by an independent and authoritative source. For example, the birth certificate on file at the Bureau of Vital Statistics would be used to verify the date and place of birth claimed on an SF 86. See "Corroborate".

Visit – 1) an assignment of either a foreign national or a U.S. national research associate, guest worker, or trainee to a training program or actively administered by a Departmental Office or Treasury bureau. 2) A visit in which the visitor will or is reasonably expected to require access to classified or sensitive but unclassified information, for which the sending company or agency must certify the visitors security clearance or favorably adjudicated background investigation to the receiving agency or company. This is referred to as "classified visit" when the visit involves access to classified information.

Visit Authorization Letter (VAL) - A letter from the security office of the sending activity to the security office of the Treasury activity to be visited, that certifies the personal information and information regarding the visitors' personnel security clearance, accesses, and/or background investigation in connection with a visit that requires access to such information. Typically used for classified visits.

Vulnerability Assessment – The process for determining whether (or not) a particular employee, facility, system, property, equipment, or activity is susceptible to an identified threat.

Waiver – See "Personnel Security – Exception".

Weapons of Mass Destruction (WMD) – Chemical, biological, radiological, and nuclear weapons.

Whole Person Concept – The basis upon which an access-granting authority makes an adjudicative determination of an individual's eligibility for access to classified information. This concept involves the careful weighing of all available information, favorable and unfavorable, both past and present, including mitigating factors.

Working Paper - Documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention.

Write-for-Release – Writing intelligence reports to disguise sources and methods to enable distribution to customers or intelligence partners at lower security levels. Write-to-release is proactive sanitization that makes intelligence more readily available to a more diverse set of customers.

Chapter VIII
Section 2

Abbreviations

Updated
6/17/11

AA – Accrediting Authority or Adjudication Authority

ACS – Access Control System.

ADB – Asian Development Bank.

ADF – African Development Fund.

AIS – Automated Information Systems.

AISP – Acquisition and Industrial Security Program.

ANACI – Access National Agency Check and Inquiries.

ATF – former Treasury bureau, the Bureau of Alcohol, Tobacco and Firearms.

BEP – Bureau of Engraving and Printing.

BI – Background Investigation

BPD – Bureau of the Public Debt.

BSC – Building Security Committee.

C & A – Certification and Accreditation.

CAGE – Commercial and Government Entity.

CAPCO – Controlled Access Program Coordination Office.

CCTV – Closed Circuit Television.

CD – Compact Disc.

CDN – Consolidated Data Network.

CFR – Code of Federal Regulations.

CI – Counterintelligence.

CIA – Central Intelligence Agency.

CI/KR – Critical Infrastructure Key Resources.

CIP – Critical Infrastructure Protection.

CM – Countermeasures.

CNACI – Child Care National Agency Check with Inquiries.

CO – Contracting Officer.

COMSEC – Communications Security.

COTR – Contracting Officer's Technical Representative. See COR.

CSA – Cognizant Security Authority.

CSO – Cognizant Security Office.

CTTA – Certified TEMPEST Technical Authority.

CVS – The Office of Personnel Management operated Clearance Verification System.

DAS – Deputy Assistant Secretary.

DBA – Database Administrator.

DCI – Director of Central Intelligence.

DCID – Director of Central Intelligence Directive.

DCII – Defense Clearance and Investigations Index.

DCS – Defense Courier Service.

DHS – Department of Homeland Security.

DIDO – Designated Intelligence Disclosure Official.

DISCO – Defense Industrial Security Clearance Office.

DNI – Director of National Intelligence.

DOD – Department of Defense.

DSO – Designated Security Official.

DSS – Defense Security Service with respect to the Department of Defense; the Diplomatic Security Service with respect to the Department of State.

DTAR – Department of Treasury Acquisition Regulation.

EAP – Emergency Action Plan or Employee Assistance Program.

EBRD – European Bank for Reconstruction and Development.

ENAC – Expanded National Agency Check.

EO – Executive Order.

EOD – Enter-on-Duty.

FAM – Foreign Affairs Manual issued by the Department of State.

FAR – Federal Acquisition Regulation issued by the General Services Administration.

FBI – Federal Bureau of Investigation.

FCL – Facility Security Clearance under the National Industrial Security Program.

FGI – Foreign Government Information.

FI – Foreign Intelligence.

FinCEN – Financial Crimes Enforcement Network.

FISMA – Federal Information Security Management Act.

FLETC – former Treasury bureau, the Federal Law Enforcement Training Center.

FMS – Financial Management Service.

FOCI – Foreign Ownership, Control, or Influence.

FOIA – Freedom of Information Act.

FPS – Federal Protective Service.

FRD – Formerly Restricted Data.

FRUS – Foreign Relations of the United States issued by the Department of State.

GCA – Government Contracting Activity.

GETS – Government Emergency Telecommunications Service.

GSA – General Services Administration.

HR – Human Resources.

HSAS – Homeland Security Advisory System.

HTML – Hyper Text Markup Language

IADB – Inter-American Development Bank.

IC – Intelligence Community.

ICD – Intelligence Community Directive.

ID – Identification.

IDRS – Integrated Data Retrieval System.

IDS – Intrusion Detection System.

IMF – International Monetary Fund; one of several international financial institutions.

IRC - Interagency Referral Center.

IRTPA – Intelligence Reform and Terrorism Prevention Act of 2004.

IRS – Internal Revenue Service.

IS – Information System.

ISC – Interagency Security Community established by Executive Order 12977 and chaired by the General Services Administration.

ISCAP – Interagency Security Classification Appeals Panel.

ISOO – Information Security Oversight Office, National Archives and Records Administration.

JPAS – Joint Personnel Adjudicative System.

LAA – Limited Access Authorization.

LAC – Local Agency Check.

LAN – Local Area Network.

LBI – Limited Background Investigation.

LCD – Liquid Crystal Diode.

LPR- Lawful Permanent Resident.

MBI – Minimum Background Investigation.

MBI/LBI – Minimum Background Investigation/Limited Background Investigation.

MOA – Memorandum of Agreement.

NAC – National Agency Check.

NACI – National Agency Check and Inquiry.

NACLC – National Agency Check with Local Agency Checks and Credit Check.

NCIC – National Crime Information Center.

NCPC – National Capital Planning Commission.

NCIX – National Counter-Intelligence Executive.

NCTC – National Counter-Intelligence Center.

NDA – Non-Disclosure Agreement.

NDC – National Declassification Center

NID – National Interest Determinations.

NISP – National Industrial Security Program.

NISPOM – National Industrial Security Program Operating Manual.

NSA/CSS – National Security Agency/Central Security Service.

NSC – National Security Council.

NSI – National Security Information.

OADR – Originating Agency's Determination Required (now obsolete marking).

OCA – Original Classification Authority.

OCC – Comptroller of the Currency.

OCIO – Office of Chief Information Officer.

ODNI – Office of the Director of National Intelligence.

OIA – Office of Intelligence and Analysis.

OIG – Office of Inspector General.

OMB – Office of Management and Budget.

OPF – Official Personnel Folder.

OPM – Office of Personnel Management.

OPM-FIS – Office of Personnel Management-Federal Investigative Services.

OPR – Office of Primary Responsibility.

OPSEC – Operations Security.

OSD – Office of the Secretary of Defense.

OSP – Office of Security Programs.

OSPD – Overseas Security Policy Board.

OSS – Office of Senate Security.

OTS – Office of Thrift Supervision.

PAA – Principal Accrediting Authority.

PBS – Public Building Service.

PCL – Personnel Security Clearance.

PCC – Policy Coordinating Committee.

PDD – Presidential Decision Directive.

PDD/NSC – Presidential Decision Directive/National Security Council.

PED – Portable Electronic Device.

PII – Personally Identifiable Information.

PL – Public Law.

PO – Program Office.

POC – Point-of-Contact.

PR – Periodic Re-investigation.

PRI – Periodic Reinvestigation.

PSQ- Personnel Security Questionnaire.

RAA – Restricted Access Area.

RAC – Remote Archives Capture project

RD – Restricted Data.

SAO – Senior Agency Official for purposes of Executive Order 13526 and having responsible for Treasury's information security program.

SAP – Special Access Program.

SAR – Special Access Required.

SBU – Sensitive But Unclassified.

SCI – Sensitive Compartmented Information.

SCIF – Sensitive Compartmented Information Facility.

SCG- Security Classification Guide.

SES – Senior Executive Service.

SF – Standard Form.

SIGTARP – Special Inspector General for the Troubled Asset Relief Program.

SII – Security/Suitability Investigations Index or Special Investigative Inquiry.

SLTPS - State, Local, Tribal and Private Sector.

SOIC – Senior Official of the Intelligence Community.

SOP – Standard Operating Procedure.

SPB – former Security Policy Board.

SPC – Security Point-of-Contact.

SSBI – Single Scope Background Investigation.

SSBI-PR – Single-Scope Background Investigation-Periodic Reinvestigation.

SSO – Special Security Officer.

STAS – Security and Threat Advisory System.

STE – Secure Telephone Equipment.

STU III – Secure Telephone Unit.

SWA- Secure Working Area.

TARP – Troubled Asset Relief Program.

TCS – Treasury Communications System.

TD – Treasury Directive.

TD F – Treasury Department Form.

TD P – Treasury Directive Publication.

TFI – Office of Terrorism and Financial Intelligence.

TIGTA – Treasury Inspector General for Tax Administration.

TO – Treasury Order.

TS – Top Secret.

TSA – Transportation Security Administration.

TSWA – Temporary Secure Working Area.

TSCO – Top Secret Control Officer.

TSCM – Technical Surveillance Countermeasures.

TSDN – Treasury Secure Data Network.

TTB – Alcohol and Tobacco Tax and Trade Bureau (TTB).

UL – Underwriters Laboratory.

US or U.S. – United States.

USC – United States Code or United States Citizen.

U.S.C. – United States Code.

USCS – former Treasury bureau, the United States Customs Service.

USSS – former Treasury bureau, the United States Secret Service.

VAL – Visit Authorization Letter.

VCSP – Visiting Contractor Security Plan.

VCSP/CI – Visiting Contractor Security Plan for Classified Information.

WMD – Weapon(s) of Mass Destruction.