Description of document:	Department of Commerce Manual of Security Policies and Procedures, 2012-2016
Requested date:	07-November-2016
Released date:	07-February-2017
Posted date:	29-May-2017
Source of document:	Department of Commerce Departmental Freedom of Information Officer Office of Privacy and Open Government 14th and Constitution Avenue NW Mail Stop 52010FB Washington, DC 20230 Fax: 202-482-0827 FOIAonline system

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

FEB 07 2017

RE: Freedom of Information Act (FOIA) Request DOC-OS-2017-000153

This letter is in response to your FOIA request to the Department of Commerce (Department), submitted on November 7, 2016, wherein you requested "a copy of the releasable portions of the Dept of Commerce OSY Security Manual." A copy of the full details of your request is enclosed.

A search of records and files maintained by OSY provided one responsive document (366 pages) which is being release in its entirety.

You have the right to appeal this FOIA request response. An appeal must be received by the Assistant General Counsel for Administration (Office), Room 5898-C, Department of Commerce, 14th and Constitution Avenue, N.W., Washington, D.C. 20230, within 30 calendar days of the date of this letter. Your appeal may also be sent by e-mail to FOIAAppeals@doc.gov or by facsimile (fax) to 202-482-2552.

The appeal must include a copy of the original request, this response to the request and a statement of the reason why you believe this response was in error. The submission (including e-mail and fax submissions) is not complete without the required attachments. The appeal letter, envelope, e-mail subject line, and fax cover sheet should be clearly marked "Freedom of Information Act Appeal." The e-mail, fax machine, and Office are monitored only during normal business days/hours (8:30 a.m. to 5:00 p.m., Eastern Time, Monday through Friday). FOIA appeals posted to the e-mail box, fax machine or Office after normal business hours will be deemed received on the next normal business day.

If you have questions concerning this response, please contact Kate McPhail at 202-482-0106 or via email at kmcphail@doc.gov.

Sincerely,

Thomas R. Predmore
Director for Security

U.S. DEPARTMENT OF COMMERCE

Manual of Security Policies and Procedures

OFFICE OF SECURITY
OFFICE OF ADMINISTRATION
OFFICE OF THE SECRETARY

Washington, D.C.
December 2012

Foreword

The Manual of Security Policies and Procedures (Manual) is issued under the authority of Departmental Administrative Order (DAO) 200-0, Department of Commerce (Department) Handbooks and Manuals, and has the same status as a DAO. It provides procedures and recommendations for reducing the risk and vulnerabilities to Department personnel, facilities and assets from potential terrorist attacks, espionage, criminal events, workplace violence, and natural disasters. The Manual applies to all bureaus and operating units within the Department.

Section I outlines Security Administration in the Department and focuses on security authorities, responsibilities, applications, and security education and awareness. Section II prescribes the policies, procedures, and standards that govern personnel security and the granting of eligibility for access to Classified National Security Information (NSI). Section III implements federal laws and regulations concerning security standards and safeguards to protect NSI. Section IV prescribes the policies, procedures, and standards that govern the implementation of physical security measures designed to protect personnel, facilities, property, and information. Section V provides guidance on protection of sensitive but unclassified information and other security matters. A Glossary provides security acronyms, terms, and definitions.

This Manual is effective immediately. All measures that protect Departmental assets and personnel from terrorist attacks, espionage, criminal events, workplace violence, and natural disasters, whether or not they are specifically included in this Manual, should be implemented, consistent with any local security requirements identified by senior managers as appropriate. The heads of Department components may issue supplementary instructions when necessary to provide for unique requirements within their organizations.

Planning for security is a management responsibility and shall be an integral part of any function or project undertaken in the Department. Heads of operating units and Departmental offices are responsible for ensuring the security of the personnel, property, facilities, and information in their respective organizations in accordance with applicable laws, regulations, executive orders, and directives. The Director for Security provides security advice, assistance, guidance, consultation, and services to assist heads of operating units and Departmental offices in performing their security responsibilities.

Release of this Manual to the public is subject to approval by the Department Assistant Secretary for Administration. E.O. 13526 - Classified National Security Information shall govern disclosure of this document to foreign officials. Applicable portions of the Manual may be released to foreign nationals employed by the Department to provide them with appropriate guidance on protection measures.

Submit recommended changes or receive additional information by contacting the Office of Security Project Management Division at 202-482-4544, or pmo@doc.gov.

Manual of Security Policies and Procedures
Table of Contents

SECTION III. CLASSIFIED NATIONAL SECURITY INFORMATION

SECTION I. SECURITY ADMINISTRATION

Chapter 1. Security Authorities and Application

1.1. PURPOSE

This Manual of Security Policies and Procedures (Manual) implements the policies and procedures that govern management and administration of threat, including personnel, information, industrial and physical security programs in the Department of Commerce (Department). These security programs are established to protect the Department's mission, people, facilities, property, activities, information, information technology systems, and all other assets of the Department. The Manual also provides guidance concerning emergency readiness and other security-related activities and functions.

1.2. AUTHORITY

The Manual is issued under the authority of Department Administrative Order (DAO) 200-0, Department of Commerce Handbooks and Manuals, and has the same status as a DAO. Selected laws, regulations, Executive Orders (E.O.), and directives pertaining to the security of personnel, facilities, and information in the Department are indicated below.

- E.O. 10450, as amended by E.O's 10491(October 1953), 10531 (May 1954), 10548 (August 1954), 10550 (August 1954), 11605 (July 1971), 11785 (June 1974) and 12107 (December 1978), Security Requirements for Government Employment, April 1953
- National Security Decision Directive (NSDD) 298, National Operations Security Program, January 22, 1988
- Presidential Decision Directive (PDD)/National Security Council (NSC) 12, Security Awareness and Reporting of Foreign Contacts, August 1993
- NSDD 189, National Policy on the Transfer of Scientific, Technological and Engineering Information, September 1985
- E.O. 12333, as amended, United States Intelligence Activities, December 1981
- E.O. 12656, Assignment of Emergency Preparedness Responsibilities, November 1988
- E.O. 12829, as amended by E.O. 12885 (December 1993), Industrial Security, January 1993
- E.O. 12968, as amended in part by E.O. 13467 (June 2008), Access to Classified Information, August 1995
- E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 2008
- Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (32 Code of Federal Regulations (CFR) Part 147)
- E.O. 13526, Classified National Security Information (NSI), December 2009
- Implementing Directive for E.O.13526, Classified NSI
- E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 2011

- Part 731, Suitability; Part 732, National Security Positions; and Part 736, Personnel Investigations, of Title 5 of the CFR
- Oaths to witnesses (5 U.S.C. § 303)
- Suspension and Removal (5 U.S.C. § 7532)
- Requirement for background checks for employees providing childcare services in federal facilities (42 U.S.C. § 13041)
- Procedures governing access to classified information (50 U.S.C. § 435)
- Classification, Declassification, and Public Availability of Classified NSI (15 CFR Part 4a, as amended July 2011)
- Loss, possible compromise or unauthorized disclosure of classified information (32 CFR § 2001.47)
- Disclosure of classified information (18 U.S.C. § 798)
- Unauthorized removal and retention of classified documents or material (18 U.S.C. § 1924)
- Offenses concerning communication of classified information by a government officer or employee to an agent or representative of a foreign government (50 U.S.C. § 783)
- Invention Secrecy Act of 1951, as amended (35 U.S.C. § 181–188)
- Atomic Energy Act of 1954, as amended (Public Law 83-703, as amended), which appears generally as 42 U.S.C. § 2011 et seq
- Requirements for the protection of safeguards information (providing safeguards for the protection of nuclear energy classified and restricted data [RD]) (10 CFR 73.21) and specific requirements (10 CFR 73.22)
- Intelligence Community Directive (ICD) 101 – Intelligence Community Policy Systems (Effective January 2009, as amended June 2009), Security Policy for Sensitive Compartmented Information (SCI) and Security Policy Manual, March 1995
- ICD 705 – SCI Facilities (Effective May 2010)
- ICD 503 – Intelligence Community Information Technology Systems Security Risk Management Certification and Accreditation (Effective September 2008)
- ICD 704 – Personnel Security Standards and Procedures Governing Eligibility for Access to SCI and Other Controlled Access Program Information (Effective October 2008)
- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 2004
- Presidential Policy Memorandum for Executive Departments and Agencies, Upgrading Security at Federal Facilities, June 1995
- Interagency Security Committee (ISC) Facility Security Determinations for Federal Facilities, April 2010
- ISC Design Basis Threat Report, November 2011
- ISC Physical Security Criteria for Federal Facilities, April 2010
- Physical protection and building security (41 CFR 101–20.103)
- Childcare centers for federal workers and allotment of space in federal buildings (40 U.S.C. § 590)

- "Child Care Center Design Guide," PBS 3425-13, U.S. General Services Administration (GSA), June 1998
- Conduct on federal property (41 CFR 101-20.3)
- Possession of firearms and dangerous weapons in federal facilities (18 U.S.C. § 930)
- Powers of marshals and deputies (18 U.S.C. § 3053)
- Law enforcement authority of Secretary of the Department of Homeland Security (DHS) for protection of public property (40 U.S.C. § 1315), as amended November 2002.
- U.S. GSA, Contract Guard Information Manual, April 2001
- Compliance with nationally recognized codes (40 U.S.C. § 3312)
- Fire safety systems in federally assisted buildings (15 U.S.C. § 2227)
- Fire Protection (Fire Safety) Engineering (41 CFR 101–6.6)
- Safety and Environmental Management (41 CFR 102–80)
- U.S. GSA, General Reference Guide for Real Property Policy, October 2010
- National Fire Protection Association (NFPA), Publication 10, Standard for Portable Fire Extinguishers, 2010 Edition
- NFPA, Publication 101, Life Safety Code, 2012 Edition
- NFPA, Publication 914, Code for Fire Protection of Historic Structures, 2010 Edition
- NFPA, Publication 5000, NFPA Building Construction and Safety Code, 2012 Edition
- National Security Presidential Directive 51/Homeland Security Presidential Directive 20, National Continuity Policy, May 2007
- National Response Framework, January 2008
- National Disaster Recovery Framework, September 2011
- Federal Continuity Directive 1, Federal Executive Branch Continuity Program and Requirements, February 2008
- Federal Continuity Directive 2, Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process, February 2008
- National Continuity Policy Implementation Plan, August 2007
- National Communication System Directive 3 – 10, Minimum Requirements for Continuity Communications Capabilities, July 2007
- National Incident Management System, March 2004
- National Stategy for Pandemic Influenza, November 2005
- National Strategy for Pandemic Influenza Implementation Plan, May 2006
- Federal Protective Service Occupant Emergency Plan, Development, Implementaiton, and Maintenance, November 2007
- PPD 1, Organization of the National Security Council System, February 2009
- PPD 8, National Preparedness, April 2011
- Department Organization Order (DOO) 10-5, Chief Financial Officer and Assistant Secretary for Administration, January 2011
- DOO 20-6, Director for Security, October 2008

- DAO 202-731, Position Sensitivity for Personnel Suitability and Personnel Security Purposes, November 1989
- DAO 202-751, Discipline, August 1980
- DAO 206-5, Occasional Use of Public Areas in Public Buildings, February 2008
- DAO 207-1, Security Programs, September 2010
- DAO 207-9, Monitoring Conversations, March, 2008
- DAO 207-10, Inspector General Investigations, October 2006
- DAO 207-11, Official Credential and Badge, July 2008
- DAO 207-12, Foreign National Visitor and Guest Access Program, April 2006
- DAO 210-1, Emergency Readiness for Departmental Continuity, November 2009
- DAO 210-7, Commerce Responsibilities in Disasters, April 1977

1.3. DELEGATION OF AUTHORITY

DOO 10-5, Chief Financial Officer and Assistant Secretary for Administration, authorizes the position of Director for Security (Director). DOO 20-6, Director for Security, designates the Director as the "senior agency official" responsible for directing and administering security programs in the Department. The Director also heads the Office of Security (OSY). The duties and responsibilities of the Director include, but are not limited to, the activities and functions listed below.

A. The Director has Department-wide staff management responsibility for establishing policies and procedures for personnel security; industrial security; the safeguarding of classified and sensitive documents and information; protection of Department personnel, facilities, property, assets and activities; identification, assessment and management of threats; security risk assessments; emergency actions and preparedness; communications security; operations security; security education, awareness, and training; and compliance with security policies and procedures.

B. The Director will provide security services when it is more practical or economical to consolidate them at the Department level, and shall provide services in the functional areas, above, as required by the Office of the Secretary and all Department organizations and personnel

1. Establish and maintain a Departmental "Occupant Emergency Program" in accordance with applicable laws and regulations.
2. Serve as the principal official responsible for coordinating and assisting in the establishment and continuity of a Department-wide emergency preparedness program.
3. Serve as the Department's liaison with federal, state, and local government agencies and organizations regarding security matters, executive protection, Departmental counterintelligence (CI) issues.
4. Conduct investigations under the authorities, functions, and responsibilities of OSY.

5. Establish and maintain a Security Council including membership identified in the established Council Charter.

C. The Director shall be responsible to:

1. Ensure effective implementation of E.O 13526, Classified NSI, as the senior agency official designated by the Secretary of Commerce under the provisions of Section 1.3. (a)(2) of that Order, concerning the authority to classify and protect NSI in the Department.
2. Ensure effective implementation of E.O. 12968, Access to Classified Information, or successor policy, as the senior agency official designated by the Secretary of Commerce under the provisions of Section 6.1. (a) of that order, concerning the eligibility for access to Classified NSI.
3. Ensure effective implementation of NSDD 298, National Operations Security Program, or successor policy, as the Departmental planner for Operations Security.
4. Ensure effective implementation of E.O. 12829, National Industrial Security Program, January 1993 or successor policy, as senior agency official to direct and administer the Department's implementation of and compliance with the National Industrial Security Program.
5. Ensure effective implementation of E.O. 10450, Security Requirements for Government Employees, April 27, 1953, and 5 CFR Part 732, National Security Positions, and their successor policies, as the senior agency official designated by the Secretary of Commerce.
6. Ensure effective support of the National Foreign Intelligence Program as required by E.O. 12333, United States Intelligence Activities, December 4, 1981, Section 1.6.
7. Ensure effective support for implementation of ISC directives under the auspices of E.O. 12977.

1.4. STATUS AND APPLICABILITY OF THE SECURITY MANUAL

A. The Manual establishes security policies and provides procedural guidance for the effective administration of security programs in the Department. The provisions of the Manual apply to all Departmental operating units, offices, facilities, employees, contractors and associates, and others who have access to Departmental facilities, information, personnel, or IT systems.

B. The policies and procedures outlined in the Manual take precedence over the security policies of any operating unit, bureau, or office in the Department; however, nothing in these regulations shall be construed as contrary to the provisions of any statute or federal regulation. In the event of a conflict, specific statutory provisions shall apply.

C. The senior official or manager of each operating unit, office, or facility in the Department is responsible for the safety and security of all personnel, property, and information under his or her jurisdiction. In addition, the Manual prescribes specific security responsibilities for managers, supervisors, and employees. Employees and other personnel associated with the Department shall report all incidents or conditions contrary to these requirements stated in the Manual to their Security Contact, Servicing Security Office (SSO), or the Director.

D. Failure to comply with the Department's security policies, procedures, or regulations may result in a written notice of violation and other administrative action as appropriate, including revocation of security clearance or removal from Federal Government service. Violations of any law or regulation may result in disciplinary action based on DAO 202-751, Discipline. If an employee violates a criminal statute, the matter may be referred to the United States Attorney's Office by the OSY for appropriate disposition or where required, shall be reported to the Office of Inspector General or other entity with appropriate jurisdiction.

1.5. ISSUANCE OF THE SECURITY MANUAL

The Manual is issued by OSY and is available electronically on the OSY's Departmental intranet site at http://home.commerce.gov/osy. Revisions to the Manual will be posted periodically on the intranet as appropriate.

1.6. INTERPRETATION

Any question concerning interpretation of the provisions of the Manual and all recommendations for changes to security policies and procedures in the Manual should be referred to the Director through an operating unit's SSO.

1.7. SUPPLEMENTARY REQUIREMENTS AND GUIDANCE

The Director will review any supplemental policies, procedures, and other forms of written guidance developed by an operating unit prior to issuance of such supplementary material. The review will determine appropriateness, technical accuracy, and compliance with laws, federal regulations, and the Department policies and procedures.

1.8. REQUESTS FOR EXCEPTION TO POLICY OR PROCEDURE

All requests for exceptions to the security policies and procedures in the Manual must be made to the OSY. Requests for all exceptions must be in writing and provide an adequate alternative for safeguarding or affording equivalent protection for all affected personnel, property, or facilities, property, information, or other Departmental assets.

1.9. EFFECT ON OTHER ORDERS

This Manual supersedes all previous security manuals governing security administration in the Department.

Chapter 2. Security Responsibilities

2.1. SECURITY PLANNING

Planning for mission critical security is a management responsibility and shall be an integral part of any function or project undertaken in the Department of Commerce (DOC). The most efficient and cost-effective method of instituting security measures for any facility or operation is through advance planning and continuous monitoring throughout the project, program, or activity. Once the essential security measures are determined, implementation of the measures is monitored to ensure the desired intent. Selecting, constructing, or modifying a facility without considering the security implications of employee safety and asset protection can result in costly modifications or retrofitting, considerable lost time, and liability for the Department. Receiving, processing, storing, or transmitting Classified National Security Information (NSI) information without adequate safeguards could result in damage to national security interests or a compromise of information entrusted to the Federal Government. Hiring individuals without the proper background investigation could also compromise critical or key Departmental programs.

2.2. ROLES AND RESPONSIBILITIES

Executive Order (E.O.) 13526, Classified National Security Information, confers the authority to originally classify information to designated agency heads and officials. In a subsequent *Federal Register* notice, the President conferred the authority to originally classify information at the Secret classification level to the Secretary of Commerce. E.O. 13526, further directs agency heads who originate or handle NSI to designate a senior agency official to direct and administer an agency-wide security program for all operating units within that agency. Departmental Organization Order (DOO) 20-6, Director for Security, designates the Director for Security (Director) as the "senior agency official" to direct and administer the DOC program implementing E.O. 13526, under which NSI is classified, safeguarded, and declassified. In addition, E.O. 13526 prescribes the policies, procedures, and standards that govern the granting of eligibility for access to NSI. The Director establishes and oversees the process to evaluate background investigations, adjudicate issues, and grant eligibility for access to NSI for employees and other persons associated with the DOC. Besides protecting NSI and determining the eligibility for access to NSI, other laws, E.O.s, and federal regulations guide Departmental security efforts to protect Department personnel, facilities, property, information, and assets, and to promote security education and awareness programs to achieve compliance with security policies and procedures. The guidance provided below expands and supplements the responsibilities listed in DOO 20-6.

A. Director for Security.

1. The Director serves as the focal point for all security matters in the Department and has Department-wide staff management responsibility for establishing policies and procedures for personnel security; safeguarding of NSI and information; protection of Department personnel, facilities, property, information, and assets; threat analysis (TA) and security risk assessments; emergency actions and preparedness;

communications security (COMSEC); operations security; security education, awareness, and training; and compliance with security policies and procedures. The Director may approve or deny requests for exceptions to the procedural requirements of the Manual of Security Policies and Procedures (the Security Manual).

2. The Director is responsible for advising and assisting heads of operating units in performing their security responsibilities. In addition, the Director provides security services when it is more practical or economical to consolidate them at the Department level. (For the purpose of administering Departmental security programs, the Office of the Secretary is considered an "operating unit" and is subject to policy and procedural requirements levied on all other DOC units. The Director shall serve as the Security Officer for the Office of the Secretary.)

3. The Director establishes the DOC Security Council, composed of representatives from each operating unit, to coordinate security measures in the Department. Operating unit representatives communicate security requirements to their respective units, exchange security-related information, and coordinate security services. Designating an employee to assist in performing security activities will not relieve the operating unit head, senior facility manager, or servicing security officer of his or her responsibilities.

4. The Director may delegate those authorities pertaining to security matters listed in DOO 20-6 to the Deputy Director or other senior managers as appropriate.

B. Heads of Operating Units. The head of each operating unit, defined by DOO 1-1, Mission and Organization of the Department, as amended, is responsible for ensuring the security of the personnel, property, facilities, information, and assets in his or her respective organizations in accordance with applicable laws, regulations, E.O.s, and directives.

1. The head of each operating unit is responsible for developing and implementing measures to protect personnel, property, facilities, information, and assets in his or her respective organization in accordance with applicable laws, regulations, E.O.s, and directives. The head of each operating unit is responsible for implementing security policies and procedures described in this Security Manual. Servicing Security Officers will provide subject matter expertise and, as appropriate or necessary, functional support to the operating units as applicable.

2. In particular, the head of each operating unit must ensure that each position within the operating unit is designated with the appropriate position sensitivity or risk level in accordance with the position sensitivity and risk criteria set forth in the Code of Federal Regulations (CFR) 5 § 731, Suitability, and § 732 National Security Positions, Department Administrative Order (DAO) 202-731, Position Sensitivity

for Personnel Suitability and Personnel Security Purposes, and this Manual in consultation with the servicing human resources manager, shall ensure that the unit's personnel suitability matters comply with appropriate laws and regulations. In particular, the head of an operating unit must ensure that each position within the operating unit is designated with the appropriate position sensitivity or risk level in accordance with the position sensitivity and risk criteria set forth in 5 CFR § 731 and § 732, Departmental Administrative Order (DAO) 202-731, and this Security Manual.

3. The head of each operating unit shall ensure that employees in their organization receive periodic training regarding safeguarding NSI in accordance with Chapter 3, Security Awareness and Education, and Chapter 35, Sensitive and Administratively Controlled Information, of this Security Manual.

4. The head of each operating unit will appoint a senior representative to the DOC Security Council. The representatives will communicate security requirements from their respective operating units, exchange security-related information, and coordinate security services in their organizations.

C. Human Resources Managers. Human resources managers or their designees are responsible for administering the personnel suitability investigations process required within their jurisdiction in accordance with appropriate laws and regulations. Operating unit managers, in consultation and concurrence with human resources managers, are the adjudicating authorities for their respective organizations. Human resources offices shall advise the Office of Security (OSY), through the Servicing Security Officer, when they become aware of information in a suitability investigation that could cause harm to the national security interests of the United States.

D. Servicing Security Officers.

1. DOC Servicing Security Officers implement and monitor compliance with Departmental security program activities in operating units on behalf of the Director. Servicing Security Officers provide security guidance, service, and support to the bureaus, operating units, and Departmental offices under their jurisdiction; implement security policies and procedures issued by OSY; and coordinate any safeguarding requirements that specifically pertain to an operating unit with the appropriate head of an operating unit.
2. Servicing Security Officers may formulate and issue supplementary instructions for their servicing area. Each Servicing Security Officer must actively administer education and inspection programs for each office within his or her service area that processes, handles, or stores NSI.

E. Facility and Senior Office Managers. DOC facility and senior office managers are responsible for ensuring the security of the personnel, property, facilities, information, and assets in their respective facilities in accordance with applicable laws, regulations,

E.O.s, and directives. Servicing Security Officers providing client services to operating units will assist facility managers in carrying out these responsibilities.

F. Security Contacts. The head of an operating unit, Departmental office, or other Departmental organization that does not have a Security Specialist assigned as a Servicing Security Officer, will appoint a liaison to OSY to act as a security point-of-contact for all security matters in their organization. The Security Contact may perform collateral duties that involve responsibilities such as initiating and processing requests for background investigations for applicants, employees, and contractors in his or her organization; forwarding up-to-date security information to supervisors and employees in his or her organization; assisting senior facility managers in coordinating physical security risk assessments of his or her facility; assisting the head of the organization in ensuring that all persons with security clearances receive an annual refresher security briefing; and requesting assistance from OSY regarding security matters.

G. Supervisors. Supervisors are responsible for ensuring all applicable security policies and procedures are implemented in their organization.

1. Supervisors will assign risk and sensitivity designations to all positions under their authority, in accordance with position designation criteria, to ensure individuals filling those positions receive the appropriate background investigation.
2. When an employee requires access to classified NSI, the supervisor will forward a completed CD-79, Request for Security Clearance, through the Servicing Security Officer to OSY, indicating the level of clearance needed, and a statement justifying need for the access.
3. If a supervisor becomes aware of any derogative information concerning an employee that indicates continued access is no longer in the interest of the national security, he or she must notify OSY so that an inquiry or investigation can be initiated to determine the validity of the information and the need to suspend, revoke, deny, or restrict the employee's access to NSI. Chapter 13, Security Adjudication Criteria, provides examples of information used to determine an individual's eligibility for access to NSI.

H. Employees and Other Individuals.

1. Employees and other individuals associated with the Department must become familiar with pertinent security regulations. Furthermore, individuals with security clearances must comply with standards of conduct when holding positions of trust as stated in E.O. 11222, Prescribing Standards of Ethical Conduct for Government Officers and Employees, and DAO 202-735A, Employee Responsibilities and Conduct.
2. All employees and other individuals who have been given access to NSI must abide by the applicable guidance and directives concerning its maintenance and protection as prescribed in Section III, National Security Information, and Chapter 35, Sensitive and Administratively Controlled Information.

3. Each employee and other individuals will advise their supervisor, Servicing Security Officer, or operating unit's Security Contact when they become aware of information about any Departmental employee or individual associated with the Department who could potentially cause damage to the national security interests of the United States.

2.3. ADMINISTRATIVE AND JUDICIAL ACTION

Failure to comply with the policies or procedures set forth in this Security Manual may result in written notice of violation and other administrative action, as appropriate, under the provisions of applicable statutes, E.O.s, and regulations. OSY shall recommend disciplinary action based on DAO 202-751, Discipline, against any employee or contractor in the Department determined to have been responsible for violation of applicable policies or procedures. Actions by an employee or contractor that indicate a disregard for the national security as determined by OSY may result in suspension and/or revocation of the individual's security clearance and possible referral for criminal proceedings.

2.4. AFTER-HOURS SECURITY CHECKS AND SELF-INSPECTIONS

Servicing Security Officers and Security Contacts, in consultation with local office managers, will conduct periodic, after-hours checks and self-inspections of areas that handle, process, and store NSI to ensure that the inspected organization complies with Departmental security policies and procedures. OSY shall conduct a continuous after-hours security inspection program to ensure compliance in each operating unit. This will include office areas within OSY.

Chapter 3. Security Awareness and Education

3.1. Security Awareness and Education

A security program is most effective when employees practice security daily. Servicing Security Offices (SSOs) and Security Contacts in an operating unit or office will develop, implement, and administer an ongoing security education and awareness program for all personnel under their jurisdiction. Supervisors are responsible for ensuring that employees fully participate in the program.

A. Security Education and Awareness Programs.

1. The security education and awareness program in each operating unit or office should address security in a positive manner. Because many aspects of security apply directly to employees, the heads of operating units and SSOs should emphasize an employee's personal responsibilities in proper security practices. These responsibilities include crime prevention and protection of Departmental assets as well as classified national security information (NSI). Law enforcement units from the local community are valuable resources to assist in this effort.
2. The security education and awareness program should include the following elements:
   a. Active, continuing participation by each unit's SSO and Security Contacts.
   b. Direction, guidance, and support provided by the head of each operating unit.
   c. Security awareness training for all new employees and on-site contract personnel.
   d. Periodic security awareness presentations to employees and contractors.
   e. Distribution of security reminders such as posters, pamphlets, and checklists.
   f. Updated security guidance and directives, as appropriate.
3. The security education and awareness program should include information on recent incidents involving security deficiencies or violations, areas of laxity, or trends that have become apparent in the security posture of the operating unit, office, or local facility, such as an increase in thefts or security violations.

B. Applicability. Executive Order (E.O.) 13526, Classified National Security Information, ensures that the standards pertaining to information security are binding on all Executive Branch departments and agencies that create or handle NSI. Pursuant to E.O. 12829, the National Industrial Security Program Operating Manual (NISPOM) prescribes the security requirements, restrictions, and safeguards applicable to industry, including security education and awareness training for contractors. The standards established in this Security Manual are consistent with the standards prescribed in E.O.13526 and the NISPOM.

C. Responsibility. The Director for Security (the Director) has overall responsibility for the Department of Commerce (Department) security education and awareness program. The SSO of each operating unit and Departmental office shall assist the Director in carrying

out this responsibility. SSOs must ensure that initial, refresher, and termination security briefings are conducted on a regular basis. Within the first 60 days of entry on duty with the Department, each individual shall attend a general security orientation briefing. An employee who is approved for access to NSI must also be briefed on the inherent responsibilities and proper procedures for handling NSI and must execute a Classified Information Nondisclosure Agreement, SF-312 before being granted a security clearance. Upon termination of the individual's security clearance by separation, transfer, or change of duties, each employee shall receive a security debriefing explaining the continuing responsibility to protect NSI.

D. Approach. Security education and awareness training should be tailored to meet the specific needs of the Department's security program and the specific role employees are expected to play in that program. The Director shall determine the means and methods for providing security education and awareness training. Training methods may include briefings, interactive videos, dissemination of instructional materials, and other media and methods.

E. Frequency.

1. Employees approved for access to NSI shall receive an annual NSI refresher security briefing.

2. The frequency of agency security education and awareness training will vary in accordance with the needs of an organization's security classification program. Each Departmental organization shall provide some form of refresher security education and awareness training at least annually for each person who has been granted a security clearance.

3.2. SECURITY BRIEFINGS

A. Coverage. The Department maintains a formal security education and awareness training program that provides for initial, refresher, and termination briefings, for individuals granted access to NSI. This chapter establishes security education and awareness training standards for original classification authorities (OCAs), security specialists, and all other personnel whose duties involve the creation or handling of NSI. These standards are not all-inclusive. The Director may expand or modify the coverage provided in this Security Manual according to program and policy needs. All Departmental personnel with a security clearance shall receive initial training on basic security policies, principles, and practices. Such training will be provided in conjunction with the granting of a security clearance but must be completed before an individual being given access to NSI. The following briefings will be required for an employee who has been granted eligibility for access to NSI.

1. **Initial EOD Briefing.** A general security orientation briefing is required for all employees, regardless of their position sensitivity or risk designation, within the first 60 days of employment. This briefing will cover basic security issues such as identification, keys, access control during and after normal work hours, office

security and crime prevention, vehicle and visitor controls, property accountability, suspicious package inspection procedures, and emergency evacuation procedures. This briefing must also cover proper usage of information technology (IT). Proper computer and Internet/intranet usage must be clearly understood and adhered to by all employees. This briefing can be provided by the operating unit or SSO, a representative from the human resources office, or the employee's first-line supervisor.

2. **National Security Education Briefing.** Employees who are approved and cleared for access to NSI must be briefed on their responsibilities with respect to possession of a security clearance and proper procedures for handling NSI. Individuals must execute a Classified Information Nondisclosure Agreement, SF-312 before being granted a final security clearance. No individual will have access to NSI until he or she has received the NSI Briefing by the SSO and has signed the SF-312. This briefing will include responsibilities of the employee prior to his or her transfer, separation, administrative downgrade of clearance, or change of duties. The Office of Security (OSY) headquarters conducts these briefings monthly and accepts all employees approved for access to NSI. Operating unit Security Contacts or SSOs may schedule cleared employees for this monthly briefing by coordinating directly with OSY.

3. **Annual Security Refresher Briefing.** Annually, employees cleared for access to NSI will receive a refresher briefing covering their security responsibilities. Such employees are required to receive this briefing at least once a year or more frequently, if required. Each operating unit or Departmental office may schedule cleared employees for the monthly security briefing provided by OSY headquarters.

4. **Original Classification Authority Training.** All OCAs must receive training in proper classification (including the avoidance of over-classification) and declassification as provided in E.O. 13526 and its implementing directives at least once a calendar year. Such training must include instruction on the proper safeguarding of NSI and on the sanctions of the order that may be brought against an individual who fails to classify information properly or protect NSI from unauthorized disclosure. OCAs who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official of the order until such training has taken place. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

5. **IT (Computer) Security Briefings.** The proliferation of computers and office automation devices presents vulnerabilities and potential threats to the protection of U.S. Government information. IT security briefings must be provided for all incoming personnel by the IT security staff. This briefing can be incorporated into

the initial EOD Security Orientation Briefing or the operating unit's general office briefing in coordination with IT security personnel. Information regarding computer security (e.g., classified data processing and protection of IT media and passwords) shall be covered in these briefings. IT security briefings must be provided to personnel whose jobs involve processing NSI on a computer system. The Office of the Chief Information Officer and OSY share responsibility for IT security.

6. **Security Debriefing.** Upon termination of employment or contract responsibilities by separation, transfer, an administrative downgrade action, or a change in duties, each employee or other individual with a security clearance must receive a security debriefing explaining that his or her access to NSI has been removed and that he or she has a continuing responsibility to protect NSI. At the security debriefing, each individual shall sign the SF-312 acknowledging the debriefing and his or her continuing responsibility to protect NSI to which he or she had access. At a minimum, the debriefing shall contain all of the following:
   a. A reminder that NSI may not be communicated or transmitted to an unauthorized person or organization.
   b. A reminder of the penalty for unauthorized disclosure of NSI.
   c. The requirement to report to OSY or to the Federal Bureau of Investigation any attempts by unauthorized personnel to obtain NSI.
   d. The employee's assurance that all NSI has been reassigned to appropriately cleared personnel in his or her organization.

   Note: Several SSOs have faced difficulty in locating personnel who have transferred, separated, or changed duties. In such instances, the SSO or the Security Contact shall make every reasonable attempt to locate and debrief these personnel. If such an attempt is unsuccessful, the SSO or Security Contact shall annotate the SF-312 that an administrative action was taken on this employee and that the person was not present for the debriefing.

   Failure of a clearance holder to exercise the security debriefing does not release the individual from the lifetime obligation to protect NSI.

B. Special Access Briefings. Other security briefings will be administered only to those employees who have been cleared for access to special access program (SAP) activities or who require briefings on unique information such as foreign travel advisories. Generally, these briefings are conducted at the Department level or by administrators of the special programs. Employees who no longer have a need for access to a special access program will receive a security debriefing that informs them that access to the special program information has been terminated and that the employee has a continuing responsibility to protect any information to which he or she had access.

1. **North Atlantic Treaty Organization (NATO) Briefing.** The NATO security procedures are contained in the United States Security Authority for NATO Affairs, USSAN 1-69. Before gaining access to NATO information, all Department personnel shall be briefed on NATO security procedures. Only an operating unit

supervisor, SSO, or other NATO-briefed Departmental employee may conduct this briefing.

2. **Communications Security (COMSEC) Briefing.** Operating units shall arrange for individuals who require access to COMSEC equipment to be briefed on proper COMSEC procedures. The designated COMSEC Custodian or Alternate Custodians shall conduct the briefing.

3. **Other Special Access Briefings.** Individuals requiring access to Sensitive Compartmented Information (SCI) shall be given a briefing by OSY, Counterespionage Division (CED). SCI policies are contained in Director of Central Intelligence Directives. For further information concerning SAPs contact OSY, CED. Not all operating units or SSOs can conduct SCI briefings. SCI access is required for the briefer. If the operating unit or SSO is unable to conduct SCI briefings, OSY/CED should be notified to coordinate a local briefing accordingly.

C. Other Briefings.

1. **Initial Facility Orientation.** The initial facility orientation briefing will address general physical security principles such as common security hazards, building security, crime prevention, key systems or other site-specific access controls, vehicle controls, property accountability, workplace violence, and package inspection programs. Departmental and Code of Federal Regulations related to handling and safeguarding NSI and sensitive information, including reporting requirements and non-disclosure provisions must also be covered, when applicable.

2. **Crime Prevention.** A well-rounded security awareness and education program includes information on crime prevention. Employees should be encouraged to remove or minimize opportunities for crime by being aware of their environment and practicing office security. Employees should also be encouraged to report unauthorized activity, security deficiencies and violations, and safety hazards.

3. **Foreign Travel Briefing.** Operating units or SSOs are required to conduct annual foreign travel briefings outlining security and personal safety issues and reporting requirements associated with traveling abroad. This briefing shall be conducted by the operating unit or SSO for employees prior to their foreign travel for the Federal Government. If the operating unit or SSO is unable to provide an oral or online briefing, the written Defensive Foreign Travel Briefing will be made available to the traveler (http://home.commerce.gov/osy/).

Chapter 4. Operations Security

4.1. DEFINITION

Operations Security (OPSEC) is an analytical process used to deny an adversary information — generally unclassified — concerning Department of Commerce (Department) intentions and capabilities by identifying, controlling, and protecting indicators associated with Departmental planning processes or operations. OPSEC does not replace other security disciplines — it supplements them.

The Department's OPSEC program activities are designed to prevent the collection of intelligence information by hostile or adversary interests through proper identification of sensitive information, assessment and analysis of the collection threat, and recommendation of countermeasures. OPSEC strengthens the traditional security program by identifying vulnerabilities or weaknesses in the protection collectively afforded by those programs.

4.2. OPSEC THREAT ASSESSMENT

Departmental sensitive assets can be defined as data, information, technology, processes, or materials used in the execution of its mission that requires protection in accordance with Departmental policies and/or U.S. law or regulation, including any asset that has the potential to compromise or adversely impact Departmental operations if inappropriately released. Sensitive assets include but are not limited to the following: Export Administration Regulations controlled technology, International Trafficking in Arms Regulations technology, personally identifiable information, proprietary or not-for-public release data, procurement sensitive information, Classified National Security Information and Controlled Unclassified Information.

4.3. OPSEC REVIEW PROCESS

A. The following program elements shall be considered when performing an OPSEC review of a program or operational component, or as part of a security compliance review:

1. Define the critical information required to conduct or carry out the mission of the office or program.
2. Define what key elements must be protected from inadvertent, intentional, or premature disclosure.
3. Determine whether a timetable has been established for the disclosure of specific information, and if a timetable is established, how this timetable is protected.
4. Determine what the threat is, who the adversaries are, and what programs or technologies are vulnerable to the threat.
5. Determine what countermeasures shall be implemented to effectively preclude, alleviate, or minimize any known or potential threat.

B. OPSEC reviews shall be conducted for all sensitive activities and facilities whenever:

1. A facility will be constructed that will be used to process or store classified or critical information.

2. New sensitive activities are initiated, or significant changes occur to existing programs.
3. A sensitive program or activity has not been the subject of an OPSEC review, and it is determined that a potential threat or vulnerability to information may be present.

C. For assistance in conducting an OPSEC review and in developing an OPSEC Plan for an office or program activity, managers should contact their Servicing Security Office. Security specialists are available to assist program managers in completing a risk analysis and in assessing countermeasures (if any) that need to be in place. Efforts shall be made to strike a balance between cost and effectiveness of the countermeasures.

D. Senior managers in the operating units shall be briefed on the results of any OPSEC review conducted for their activities. The briefing shall include a report of any OPSEC vulnerabilities that have or have not been resolved, the exposed risk, and whether an acceptable risk remains.

4.4. YOUR PERSONAL RESPONSIBILITY

The security of Departmental information is everyone's responsibility. Employees, contactors, and anyone authorized access to Departmental information must be aware that sensitive, proprietary, or classified information can be transmitted in various ways. An adversary may attempt to target or collect sensitive information that could result in a loss for the United States and a valuable acquisition for another country. Good OPSEC practices include using secure communications when required, protecting your documents from unauthorized disclosure, and being aware of your surroundings while discussing sensitive information.

For additional information, use the following link to the Interagency OPSEC Support Staff: http://www.ioss.gov/.

Chapter 5. Security Inspections and Assistance

5.1. PURPOSE

A. Department of Commerce (Department) security policy is designed to ensure proper and adequate security services to customers while safeguarding and protecting all Departmental assets and interest from theft, sabotage, espionage, and/or hostile acts. Threats to the Department have an adverse impact on national security and threaten the health and safety of Department employees, contractors, other individuals, and the public. Security inspections, which may consist of security surveys, assessments, assistance visits, compliance reviews, and unannounced spot checks, are conducted to ensure compliance with laws, Executives Orders (E.O.s), Federal regulations, and Departmental policies.

B. This chapter provides an overview of security inspections conducted by the Office of Security (OSY) and sets standards for establishing and maintaining an ongoing self-inspection program in the operating units. Departmental policy mandates that security inspection programs shall include the periodic internal review and evaluation of individual operating unit activities with respect to the effective implementation of the classified National Security Information (NSI) Program as established under the E.O. 13526, Classified National Security Information. These standards are binding and apply to all offices that process, handle, and/or store NSI, equipment, or materials, including contractors and federal advisory committee members, pursuant to the National Industrial Security Program described in E.O. 12829.

C. The National Industrial Security Program Operating Manual (NISPOM) prescribes the security requirements, restrictions, and safeguards applicable to private industry under U.S. Government contract, including contractor-conducted self-inspections. The standards established in the NISPOM are consistent with the standards prescribed in E.O.13526.

D. The Director for Security is responsible for ensuring that all Departmental operating units comply with established security laws, regulations, and policies. To carry out this function, the OSY Information Security (INFOSEC) Program and Servicing Security Offices (SSOs) conduct compliance reviews, inspections, assessments, and spot checks.

5.2. INSPECTION PROCEDURES AND FREQUENCY OF COMPLIANCE REVIEWS

A. Inspection procedures and frequency of compliance reviews are based on program needs and the magnitude of security activity. Activities that process NSI shall conduct internal classified document reviews on an annual basis. SSOs will ensure that classified storage containers within their respective areas are inspected annually. OSY INFOSEC and SSOs will conduct NSI oversight inspections of operating units biannually.

B. The elements of the security inspection program include, but are not limited to, those noted in the following paragraphs. The scope of the self-inspection may expand according to program and policy needs. Each inspection of an operating unit's security program may involve any of the following:

1. A review of relevant security directives, guides, and instructions.
2. Interviews with key personnel, classifiers, users, and/or holders of classified materials.
3. A review of access and control records.
4. A review of internal procedures and processes pertaining to the protection, control, and safeguarding of NSI.
5. A review of Department-generated or derivative NSI that has not been reviewed during previous inspections, and a review of all NSI materials processed and/or stored by the operating unit activities.

5.3. COVERAGE OF COMPLIANCE INSPECTIONS

OSY INFOSEC and SSOs will review the security policies and procedures carried out in the various operating units to determine compliance with the Department's security programs. Elements of the security inspection program are indicated in the sections below, but are not limited to these items. Each review of a classification activity need not include all the elements covered below.

A. Original Classification.

1. OSY INFOSEC may evaluate an Original Classification Authority's (OCA) general understanding of the process of original classification, including all of the following:
   a. Applicable standards for classification.
   b. Levels of classification and the damage criteria associated with each.
   c. Required classification markings.
   d. Declassification instructions.
2. The review may determine whether delegations of OCA conform to the requirements of E.O. 13526, including whether:
   a. Delegations are limited to the minimum number necessary to effectively administer the program.
   b. Designated original classifiers have a demonstrable and continuing need to exercise this authority.
   c. Delegations are in writing and identify the official by name or position title.
3. The review may assess the OCA's familiarity with the duration of classification requirements, including all of the following:
   a. Assigning a specific date or event for declassification when possible.

b. Establishing a maximum 10-year duration of classification when an earlier date or event cannot be determined.
c. Limiting extensions of classification for specific information for successive periods not to exceed 10 years at a time.
d. Exempting specific information from declassification within 10 years, as provided in E.O.13526.

4. A review may be conducted of a random sampling of NSI generated by the inspected activity to determine the application of proper and complete markings.

5. The review team may evaluate the OCA's classification actions to determine whether they comply with the standards related to classification and declassification specified in this Manual.

6. The review may verify that OCA classification actions do not violate the prohibitions and limitations on classification.

7. The review will assess whether the OCA's procedures to challenge classification decisions meet the requirements of the E.O. 13526 and this manual.

B. Management and Oversight. Before making original classification decisions, the OCA must be trained on the proper procedures for such actions. OSY INFOSEC and SSOs will assess whether:

1. Appropriate training is provided to an OCA.

2. Senior management demonstrates an active commitment to the overall success of the security program, including providing the necessary resources for effective implementation and policy compliance.

3. Users and holders of NSI receive guidance concerning security responsibilities and requirements.

4. Effective controls are established and maintained to prevent unauthorized access to NSI.

5. Contingency plans are established and understood by all personnel responsible for safeguarding NSI during emergencies or disasters.

6. The system used to rate employees on job performance includes the management of NSI as a critical element or item to be evaluated in the rating of OCAs, security managers or officers, security specialists, classification management officers, classified control points (CCP), and other employees involved with the storing, processing, or handling NSI.

7. A defined system is in place for collecting information on the estimated costs associated with implementation of E.O. 13526 for classification and declassification related activities.

C. **Derivative Classification.** OSY INFOSEC and SSOs may assess individuals who perform derivative classification actions to determine their understanding of the following requirements:

1. Conditions for derivative classification.
2. Requirement to consult with the originator of the information when questions concerning classification arise.
3. Proper use of classification guides.
4. Proper and complete application of classification markings to derivatively classify, including the requirement that all derivative documents must carry forward all markings (including portion markings) and declassification instructions.
5. Annual training is provided to all individuals that derivatively classify information.

D. **Declassification.** OSY INFOSEC and SSOs may inspect the following declassification actions and activities:

1. The team may verify whether the operating unit/OCA has established, to the extent practical, a system of records management to facilitate public release of declassified documents.
2. The team may evaluate the status of the operating unit/OCA's declassification program, including the requirements to:
   a. Comply with the automatic declassification provisions regarding historically valuable records more than 25 years old.
   b. Declassify, when possible, historically valuable records prior to accession into the National Archives and Records Administration.
   c. Provide the Archivist with adequate and current declassification guides.
   d. Ascertain that the mandatory review program conforms to established requirements.

E. **Safeguarding.** OSY INFOSEC and SSOs may review an operating unit's NSI program to determine compliance with all of the following items:

1. Establish standards for safeguarding classified NSI.
2. Ensure controls are in place to access NSI.
3. Identify, report, and process unauthorized disclosures of NSI.
4. Maintain procedures to ensure that:
   a. The operating unit exercises proper control over the NSI it generates, processes, handles and/or stores.
   b. Holders of NSI do not disclose information originated by another agency without that agency's authorization.
   c. Departing or transferring individuals with access to NSI return all NSI in their possession to their designated CCP or other authorized, cleared agency

personnel prior to termination of security clearance and receive debriefing when required.

F. Security Education and Awareness Program. OSY headquarters may conduct compliance reviews to evaluate the effectiveness of the SSO's security education and awareness training program in familiarizing and refreshing appropriately cleared personnel with regulations, policies, and procedures concerning NSI.

Chapter 6. Incident Reporting

6.1. INCIDENT REPORTING SYSTEM

An incident reporting system is an essential element of any security program. Notification to a centralized fusion center is imperative in order to ensure that a consolidated, accurate flow of information is provided to leadership within the Department.

The rationale for timely reporting of a severe incident is to ensure that anything that occurs on/in a DOC occupied facility; impacts our personnel, visitors or contractors; or may have an impact on the performance of our mission essential functions is monitored. The timely reporting of security specific incidents increases the possibility of minimizing damage, apprehending perpetrators, and recovering property.

Procedures addressed below are divided into two specific areas: those dealing with potential criminal activity and those dealing with severe incidents relating to personnel, facilities and mission accomplishment.

6.2. REPORTING REQUIREMENTS, CRIMINAL INCIDENT

A. Departmental Personnel. *Imminent threats to life or property should be immediately reported to local law enforcement,* followed by prompt reporting to the Office of Security (OSY) Emergency Operations Center (EOC) at the telephone number (202) 482-5100, and to the appropriate Security Contact. Discovery or knowledge of unlawful, dangerous, or unauthorized practices or conditions, or a violation of security regulations, shall be reported immediately to the EOC at (202) 482-5100, followed by prompt reporting to the appropriate Security Contact.

1. Matters involving fraud, waste, and abuse should be promptly reported to the Departmental Office of Inspector General (OIG) pursuant to Department Administrative Order (DAO) 207-10. Cyber security issues should be promptly reported to the Departmental Office of the Chief Information Officer (OCIO) pursuant to Department Organizational Order (DOO) 15-23.
2. The individual reporting an incident should make notes regarding the incident in the event security or law enforcement officials request a follow-up or written report.

B. Security Contacts. Security Contacts shall immediately provide available information regarding incidents to their Servicing Security Officer, followed by a written report within three business days that provides any new information. This report should also address internal actions taken or referrals made.

Criminal incidents that occur at General Services Administration (GSA) leased, owned, or managed facilities should be reported to the facility guard force, Federal Protective Service, GSA Regional Office, *and* the Servicing Security Officer.

C. Servicing Security Officer. Servicing Security Officers should follow up on reports made by Departmental personnel and Security Contacts.

1. Follow-up reports should describe any additional information, actions taken, or referrals made, and should be submitted in writing to the EOC at eoc@doc.gov within 30 calendar days.
2. Servicing Security Officers will submit an annual summary of incidents to the EOC for the preceding calendar year by January 31. Thefts of materials valued at less than $500 may be listed by date, description of property, and location; other reporting and thefts of materials valued at more than $500 should be listed by date, description of incident, incident location, initial reporting person, and disposition.

D. EOC Duty Officers will make all internal headquarters notifications and referrals, as appropriate.

E. Servicing Security Officers, Security Contacts, and EOC Watch/Duty Officers will ensure that reporting, notifications and referrals comply with the procedures outlined in Chapter 36, Mission-Critical Threats to the Department.

F. Initial Inquiries to Support Reporting Procedures.

1. For thefts involving property valued at more than $500, or for other matters as directed by OSY, the Servicing Security Officer, Security Contact, or facility manager may perform an initial inquiry. The inquiry should objectively determine the facts of the incident, including who, what, when, where, how, and why.
2. Servicing Security Officers, Security Contacts, or facility managers will ensure that such inquiries do not interfere with the procedures outlined in Chapter 36, Mission-Critical Threats to the Department, or the efforts of other governmental investigative or law enforcement agencies.

6.3. REPORTING PROCEDURES, NON-CRIMINAL INCIDENT

A. Events vary and may include, but are not limited to:

1. Terrorist attacks (affects)
2. Severe weather events
3. Major earthquakes
4. Tsunamis
5. Major utility outages
6. Significant cyber attacks
7. Large scale transportation disruptions
8. Significant accidents/injuries or illnesses involving DOC personnel, visitors or contractors

B. These events may not directly affect the DOC facilities; however, their impact may greatly affect its employee's homes, personal safety and ability to report to work in a safe and timely manner. Notification of these incidents to the EOC may be received by,

but are not limited to, e-mails from the National Operations Center (NOC) as well as other federal information systems, alerts issued by the National Weather Service, and announcements from state and local emergency management agencies.

C. When a significant event occurs, the EOC should be notified by calling 202-482-5100 with a follow-up email to the EOC at eoc@doc.gov. This notification applies 24 hours a day, 7 days a week, 365 days a year.

6.4 EOC WATCH/DUTY OFFICER RESPONSIBILITIES

A. A Watch Officer (during the day) and a Duty Officer (after hours) monitors all traffic sent to the EOC during his/her tour of duty.

B. Upon receipt of either a criminal or non-criminal incident report he/she will make all internal headquarters notifications and referrals, as appropriate and in accordance with internal Standard Operating Procedures.

C. Notifications are made to various groups depending on the significance of the event. The identified groups represent different levels of management within the Department. The decision to raise the level of notification will be made dependent on the severity of the event.

D. The EOC will monitor the incident and continue to disseminate updates until closure of the reporting process is justified.

Chapter 7. Occupant Emergency Plans and Procedures

7.1. EMERGENCY PLANNING

A. An Occupant Emergency Plan (OEP) is an essential part of an emergency management program. Properly developed plans can reduce the risk to personnel, property, and other assets while minimizing work disruption in the event of an emergency. This chapter provides guidance for the preparation and maintenance of plans to deal with those emergency situations that could endanger personnel or affect facilities occupied by Department of Commerce (Departmental) personnel.

B. Because of the variety of size and functions of Departmental facilities, it is impractical to develop a standard OEP suitable for all offices. While this chapter prescribes guidelines and procedures to follow when preparing an emergency plan, it is essential that each plan be tailored to accommodate local conditions and requirements. Emphasis must be placed on developing a workable, realistic plan with the key emphasis being life safety. Some plans will be more elaborate than others (e.g., plans for the Herbert C. Hoover Building or the Census Bureau Data Center will be quite extensive while the plan for a small post of duty may require only a few paragraphs).

C. The OEP should provide guidance for occupants to follow in the event of an emergency to protect themselves and other personnel within the office, building, or facility. Personnel safety is the primary concern of any OEP. It is also important to protect the facility, property, equipment, and information. A range of situations must be addressed so that personnel involved in an emergency will know what to do. OEP guidelines and a checklist to assist in formulating a sound plan are provided.

D. This chapter outlines the responsibilities for emergency planning in Departmental facilities, prescribes the OEP planning process, and provides guidance for Departmental organizations to provide for the protection and safety of Departmental personnel during emergencies.

7.2. RESPONSIBILITIES

A. Department of Homeland Security (DHS). The *Occupant Emergency Plan (OEP) Guide, November 2007* requires either an OEP or an Emergency Action Plan (EAP) for virtually all government owned or leased facilities. It provides guidance pertaining to the preparation, implementation, and maintenance of OEPs in line with national preparedness efforts of the National Infrastructure Protection Plan (NIPP), National Response Plan (NRP), and National Incident Management System (NIMS). OEPs that are consistent in structure and content will enable better coordination of facility occupant emergency actions with outside authorities and first responders. Because of these requirements and in an effort to cooperate with the General Services Administration (GSA) and other tenant agencies, facility managers will follow this OEP Guide whenever possible when developing emergency plans.

B. Director for Security (Director). Under the provisions of Departmental Organizational Order (DOO) 20-6, the Director is responsible for coordinating,

establishing, and maintaining a Departmental Occupant Emergency Program for organizational units in the Department. The Director will carry out this responsibility by providing standards, guidelines, and procedures for development of comprehensive OEPs that protect all Departmental occupants and workspaces. In addition, the Director will develop a program to evaluate the OEPs in the respective operating units.

C. **Heads of Operating Units.** The head of each operating unit is responsible for ensuring the safety and security of all personnel in the operating unit. This includes the development and implementation of OEPs for each facility assigned to his or her respective unit and ensuring that development of the OEP is coordinated with the Office of Security (OSY) headquarters as well as the GSA (or other lessor) in facilities administered by another organization. A representative (i.e., Safety Officer or Director of Facilities) of each operating unit head must be delegated the authority to review the OEP for each facility under that head's purview on an annual basis to **endorse the adequacy of the OEP and training.**

D. **Facility Manager.** Each facility manager is responsible for ensuring that OEPs are developed, coordinated, and implemented to protect the personnel, property, and information at the Departmental facility they administer or support.

E. **Designated Official.** The Designated Official in each facility is responsible for coordinating development, implementation, and maintenance of the OEP of his or her site. At those facilities where the Department is the primary federal agency, the highest ranking official at the facility, or alternatively, a designee selected by mutual agreement of occupant agency officials, will serve as the Designated Official and will be responsible for coordinating development, implementation, and maintenance of the OEP. At those facilities where the Designated Official is not a Departmental employee, the Senior Department Official at that site will work with the facility's Designated Official to develop, implement, and maintain the plan. The Department's senior-level official should be an employee with sufficient knowledge to carry out the requirements of this position. This position may be delegated in writing, and the person holding the position shall retain oversight of the OEP for all Departmental occupants.

F. **Managers and Supervisors.** All managers and supervisors are responsible for cooperating with the Designated Official to implement and maintain an OEP for the facility. Managers and supervisors who have employees assigned as Emergency Response Team (ERT) members supporting the OEP will notify the Designated Official when any team member transfers, retires, or because of extraordinary work and/or circumstances, can no longer perform his or her duties as an ERT member. The manager or supervisor may identify a replacement member and notify the Designated Official of this change. The manager or supervisor will also ensure that all occupants are aware of and comply with the guidance contained in the facility's OEP.

G. **Emergency Response Team Members.** The ERT is composed of trained personnel, established to assist occupants and to perform important functions in the event of an emergency. ERT members should be identified by the Designated Official to other ERT members and the facility occupants. Individuals assigned to the ERT should be

familiar with the facility. ERT members must be capable to facilitate evacuation of the offices as well as the safe movement or assembly of occupants under their responsibility.

7.3. PLAN DEVELOPMENT

A. An effective plan includes various anticipated emergencies, and is simple to follow and implement. Complex plans are more difficult to execute and often cause confusion. The plan should be designed to eliminate confusion and provide an orderly procedure for the protection of personnel, property, information, and facilities. Life safety is the primary concern.

B. A properly developed plan requires coordination with federal, state, and local agencies that provide assistance during emergencies. For example, knowledge of procedures and techniques used by local fire and police departments and the DHS Federal Protective Service (FPS) is necessary to develop an effective plan to deal with fires, building evacuations, demonstrations, chemical and biological threats, etc. Contacts with local emergency organizations can develop awareness of local conditions that need to be addressed, such as flood, earthquake, and local severe weather hazards.

C. An OEP planning team consisting of the Designated Official, the building or facility manager, GSA personnel (if applicable), physical security specialists (if available), technical experts, safety specialists, and local first response authorities should be formed to help develop the plan and the OEP support organization. The planning team should remain available for consultation after the plan has been completed.

D. It is important that all occupant agencies and activities be involved in all aspects of planning and staffing the OEP. If there are non-government activities in the building or facility, these activities should be invited to participate in the planning and implementation process. The plan is designed to protect the life and property of all occupants, and therefore, participation by all organizations within the facility will ensure special interests and needs are considered and incorporated into the plan.

E. Provisions will be made in the plan for the facility manager to notify lessors and other tenants as necessary, if an emergency does occur, where there is possible danger to other tenants, such as a fire, water leak, discovery of an explosive device, hazardous material, etc.

F. If a childcare center is located in the facility, the Designated Official should work with the director of the facility and with GSA (if applicable) to develop and publish emergency response procedures. The childcare center procedures should be a stand-alone document, with a current copy maintained as part of the facility's OEP.

G. The GSA (if applicable) has direct responsibility for providing guidance, oversight, and assistance to childcare center staff in the development of the center's OEP. Although development of this OEP is the direct responsibility of the GSA (if applicable), facility management, safety personnel, security personnel, and DHS FPS may be asked to jointly draft, review, and agree with the plan. The childcare center's OEP shall be included in the facility's overall emergency plan.

H. This inclusion is necessary to ensure that facility management, ERTs, security and law enforcement officials are able to identify established procedures that ensure the safety of all children and staff (e.g., alternative off-site relocation space, assembly areas, and Shelter-In-Place [SIP] locations) during an emergency, and if needed, provide supplemental support.

I. Guidelines for developing an OEP are located on GSA's website at http://gsa.gov/graphics/pbs/OEP_Guide.pdf and should be coordinated between childcare center staff and the appropriate GSA office. More information concerning childcare center's OEP can be found at http://www.gsa.gov/portal/content/100898.

J. Provisions will be made in the plan to address the safety, accountability, and evacuation of persons with special needs. These provisions may be in the form of "evacuation buddies," safe rooms, etc. More information regarding emergency procedures for persons with special needs can be found in Section 7.22, Emergency Procedures for Persons with Special Needs, of this chapter.

K. The plan will identify the individual responsible (by position/title) for each action specified in the plan.

7.4. COMPONENTS OF THE PLAN

A. As each facility completes the development of an OEP, the information should be published as a directive entitled, "*OEP for (Name of Facility).*" The DHS OEP Guide allows Facility Security Level (FSL) 1 facilities to utilize GSA Form 3415, Occupant Emergency Plan (abbreviated), as their OEP.

B. An OEP is required for each individual building located on the site, campus, or facility. The OEP for each building *should be incorporated into* one larger facility plan. This will ensure that consideration is given to communications compatibility and component standards in situations where the entire campus may be affected. The senior Designated Official for the campus is responsible for oversight and compliance of the overall OEP. Those facilities meeting FSL Level I criteria as identified in Table 1, FSL—Facility Security Level Determinations for Federal Facilities may use either GSA Form 3415 to document emergency information or may opt to follow the guidelines in this chapter instead, at their discretion. FSL Level II, III, and IV facilities are required to follow the more extensive guidelines contained in this chapter.

Table 1. FSL—Facility Security Level Determinations for Federal Facilities

LEVEL	LEVEL DESCRIPTION
LEVEL I	Mission Criticality: Low. Administrative, direct service, or regulatory at a local level. Symbolism: Low. No external features or public contact readily identifying it as a U.S. Government facility. Facility Population: Less than 100. Facility Size: Less than 10,000 sq. ft. Threat to Tenant Agencies: Low. Little or no public contact, no history of demonstrations or violence at or directed at the facility.
LEVEL II	Mission Criticality: Medium. District or statewide service or regulatory operations; COOP facilities for other than national headquarters. Symbolism: Medium. Readily identified as a U.S. Government facility based on external features or on the nature of public contact; dominant, single federal facility in a community or rural area. Facility Population: Between 100 – 250. Facility Size: Between 10,001 – 100,000 sq. ft. Threat to Tenant Agencies: Medium. Generally non-adversarial public contact based on the nature of the business conducted; located in a low-crime area; history of demonstrations or violence against the tenant agency/agencies (not at facility).
LEVEL III	Mission Criticality: High. Original, irreplaceable material or information central to the daily conduct of government; designated as a shelter in the event of an emergency incident; COOP facilities for department or agency headquarters. Symbolism: High. Well-known U.S. Government facility; agency/bureau headquarters; collocated with other highly symbolic facilities. Facility Population: Between 251 –750. Facility Size: Between 100,001 – 250,000 sq. ft. Threat to Tenant Agencies: High. Public contact is occasionally adversarial based on the nature of the business conducted and routinely draws the attention of organized protest groups; located in moderate-crime area; 5–10 incidents per year requiring law enforcement response for unruly or threatening person in site.
LEVEL IV	Mission Criticality: Very High. Communications centers that support national essential government functions; houses personnel or specialized equipment necessary to identify and/or respond to large-scale or unique incidents; houses material or information that, if compromised, could cause a significant loss of life; Continuity of Government facilities. Symbolism: Very High. Popular destination for tourists; widely recognized to represent the Nation's heritage, tradition or values; executive department headquarters building. Facility Population: More than 750. Facility Size: More than 250,000 sq. ft. Threat to Tenant Agencies: Very High. Tenant mission is adversarial in nature; located in a high-crime area; more than 10 incidents per year requiring law enforcement response for unruly or threatening person in site; tenant mission is controversial and routinely draws the attention of organized protest groups.

LEVEL V	The criticality of the mission or the symbolic nature of the facility must be such that it merits a degree of protection above that specified for a FSL IV facility. As general guidance, agencies should consider any facility that is given a "Very High" score value for criticality or symbolism and is a one-of-a-kind facility or nearly so, as potentially suitable for designation as a Level V facility.

C. The plan for all Level II–V facilities will consist of an introduction describing the purpose, scope, and general content of the plan.

1. Each plan will contain the following administrative information:
   - An Approval Page signed and dated by the Approving Official.
   - An Annual Review/Update page which contains:
     - Detailed listing of all the changes made since the last review/update
     - Date of the last review/update
     - Signature of the Approving Official
2. Each plan will contain, at a minimum, an appendix for each of the following topics:
   - Map displaying both the building and adjacent areas with emergency exits, evacuation routes and assembly areas superimposed thereon
   - Building and tenant information
   - Emergency organization
   - Emergency contact numbers
   - Available emergency services
   - Evacuation/Shelter-in-Place (SIP) procedures
   - Medical assistance and rescue
   - Persons with Special Needs
   - Fire emergencies
   - Active shooter procedures
   - Bomb threats and suspicious packages
   - Hazardous Materials (HAZMAT) incidents
   - Natural disasters
   - Demonstrations and civil disorders
   - Workplace violence
   - Hostage situations and terrorist incidents
   - Reporting of suspicious activities and unlawful acts
   - Emergency communications systems
   - Safe Haven, as appropriate

D. While the OEP Guidelines require a Command Center to be identified and staffed by the Command Center Team, it is understood that not all facilities have the capability or personnel to sustain this requirement. Therefore, it is the Designated Official's responsibility to evaluate and determine whether a Command Center is required and whether it will be established. If the decision is to establish one, it becomes the centralized place for all response personnel to manage an emergency situation. (It should be noted that the local emergency responders may set up their own Command Center not collocated with the Department Center.) An off-site alternate Command Center should be considered in the event the emergency situation denies use of the

primary site. At a minimum, the Command Center does not have to be an elaborate operation, but should have the following as a minimum:

- Minimum of two telephones with separate lines or rollover capabilities
- Portable and/or wireless communication devices
- A method to communicate with occupants, i.e., public address system controls.

E. When the Designated Official is not a Departmental employee, the procedures outlined below shall be followed by the Senior Departmental Official in the facility:

1. Each office or facility occupied by Departmental personnel will have an OEP whether or not a Departmental employee is the Designated Official. If an OEP is in place at a non-Departmental facility, the Senior Departmental Official residing at that site must ensure that all Departmental occupants are included in the building's plan.
2. In facilities where the Designated Official is not a Departmental employee, the Senior Departmental Official will cooperate with the Designated Official to develop, implement, and maintain an effective OEP. Cooperation will include all of the following:
   a. Advising the Designated Official of the Department's needs and requirements.
   b. Participating in training, drills, and tests.
   c. Providing proportionate staffing for the plan.
3. The Senior Departmental Official for the facility and the bureau's Emergency and Safety Management offices will evaluate the plan to ensure that it is adequate to protect Departmental personnel and other assets. After the development of the OEP, the Senior Departmental Official and/or Designated Official can request a second review from the Servicing Security Office (SSO). The plan will be evaluated based on guidelines in this chapter. If the plan is determined to be inadequate and the non-Departmental Designated Official will not make the necessary adjustments, the Senior Departmental Official will supplement the plan as necessary. Any supplements determined to be necessary will be prepared as an appendix to the OEP and will be distributed to Departmental occupants as appropriate.

7.5. REVIEW OF OCCUPANT EMERGENCY PLANS

A. The Department's Designated Official in each DOC leased and owned facility is required to complete an annual review of that facility's OEP. In those facilities where the Designated Official is not a Departmental employee, the Senior Departmental Official (or another management-level person designated by the senior-level official) will be responsible for reviewing the facility's OEP and/or the addendum to the OEP on an annual basis. This chapter provides guidelines for developing, coordinating, and implementing an OEP. These guidelines may be used to assist the Department's Designated Official or the Department's senior-level official to conduct a self-evaluation of his or her facility's OEP or addendum to the facility's OEP.

B. The Federal Management Regulations (FMR) outlines responsibilities for the safety and security of building occupants. The head of each operating unit will identify, by title, a person within the chain of responsibility for his/her facilities who will certify the adequacy of OEP of each of those facilities.

C. As a part of their responsibility to conduct Facility Security Assessments (FSA) in designated Departmental facilities, OSY headquarters personnel will continue to review each facility's OEP program as part of the Risk Management process based on established schedules.

D. As part the Compliance Review Program, headquarters will provide periodic reports to Senior Departmental and operating unit officials on FSAs and OEPs. OSY will confer with Designated Officials to further review OEPs and assist them, as necessary, with implementing corrective actions.

7.6. OCCUPANT EMERGENCY ORGANIZATION

A. Occupant Emergency Organization. The OEP for each facility is devised to provide emergency procedures to protect life and property in federally occupied facilities and is designed to protect occupants assigned to the building or facility. All resident federal agencies assigned to the building or facility should be a part of the plan.

1. An emergency may involve fires, bomb threats, explosions, HAZMAT release, demonstrations, civil disturbances, hostage situations, floods, hurricanes, winter storms, tornadoes, power failures, and earthquakes, as well as other natural and human-caused disasters. In the event of an emergency, properly developed plans should reduce the risk to personnel, property, and other assets while minimizing work disruption.

2. The federal agency with the largest number of personnel residing in a building or facility is referred to as the primary occupant agency. As such, the highest-ranking official of the primary occupant agency is generally identified as the Designated Official having responsibility for development and maintenance of the OEP.

3. The occupant emergency organization is composed of tenant agency representatives in the building who are designated to perform OEP responsibilities. (The occupant emergency organization may also include tenants from non-federal agencies.) Emergency operations are directed by the emergency organization. The following list includes both required and recommended minimum components of an emergency organization. All components may not be necessary for every organization.
   a. **Designated Official.** The highest-ranking official of the primary occupant agency or the alternate highest-ranking official or designee selected by mutual agreement of other occupant agency officials. This official is responsible for the activation, coordination, and maintenance of the plan. After normal duty hours, the senior federal official present shall represent the Designated Official.
   b. **Emergency Operations Coordinator.** An Emergency Operations Coordinator assists and acts for the Designated Official and serves as a liaison with staff and

other team members. The Coordinator records implemented emergency procedures, maintains organization records, and provides other required administrative services, as required.

c. **Emergency Operations Teams.** Participation by the appropriate individuals within the organization is required to perform all of the following duties:

1) Identify utilities, fire protection, communications, and other emergency equipment in the building.
2) Maintain an emergency call list for utilities and hazardous substances.
3) Direct damage control team activities.
4) Make recommendations regarding use of facilities and equipment.
5) Coordinate planned movement and/or evacuation of occupants and other activities of Emergency Response Team members.
6) Assist persons with special needs, as appropriate.
7) Identify available medical emergency services, maintain first-aid equipment, and arrange CPR, first-aid, and Public Access Defibrillator (PAD) program training and/or certification.

B. Emergency Contact Numbers. All personnel in the facility should know whom to contact in case of an emergency. This information should be prominently displayed as well as published in the OEP.

C. Building and Occupant Information. The OEP should contain specific information about a building's construction, fire prevention and protection systems in place, and tenant information. This information can be provided in a narrative form or on a building information sheet. Floor plans should be included with evacuation routes clearly marked.

D. Emergency Services. The availability and response of emergency services are vital to an emergency plan. Appropriate assistance obtained rapidly will greatly minimize the effect of an emergency. The plan must identify, with telephone numbers, the services required for each emergency, as well as the capabilities, limitations, and response times of each service. In relatively small offices, these requirements will be greatly scaled down to meet the needs of the particular office.

E. Evacuation. The larger the building, the more complicated the evacuation tends to be. The evacuation procedures should provide for the fastest route(s) out of the building for all occupants. Alternate routes should also be specified in the event the primary route is not accessible. The primary goal is to move individuals from the danger area as safely and rapidly as possible.

F. Evacuation Authorization.

1. The official(s) and designated alternates authorized to order an evacuation must be specified in the plan by title. The decision to evacuate depends on the type of threat, the circumstances of the threat, and where the danger is or is suspected to be.

2. Evacuation for a fire, bomb threat, explosion, inclement weather, utility failure, or some other hazardous condition may or may not be prudent. There will be situations where a full evacuation will be automatic; however, evacuation of an entire building or area may not always be advisable or practical.

3. In many cases, a partial evacuation will be more advisable, such as when an explosive device is found in a large building or an explosion occurs in one area of a large building. In situations where a partial evacuation or SIP action is advisable, it is important that access to the hazardous area be controlled so that individuals do not inadvertently enter these areas. Partial evacuations or SIP actions are addressed in this chapter.

G. Evacuation Signals.

1. The method of notifying occupants to evacuate will vary depending on the building layout and alarm system installed but must be specified in the plan. The general alarm can and should normally be used for complete evacuation.

2. Emergencies such as fire, bomb and bomb threat, suspicious package, explosion, gas leak, power failure, etc., may require following different procedures.

3. Good communications are necessary to get official notification to the proper people to avoid confusion. Volunteers that act as ERT members should be assigned to each building. ERT members will assist emergency management personnel in the event of an evacuation or SIP event. These trained personnel can provide invaluable assistance and ensure more effective communications occur during the event. ERT members may also be called upon to assist persons with special needs or visitors who may be unfamiliar with the building or require assistance during evacuations or a SIP. The ERT members must know which procedure to use so that the occupants can be quickly notified and directed to the proper location. ERT members should be clearly identified (e.g., armbands, colored vests, etc.), so that all emergency personnel and individuals that may require assistance know who to contact during an emergency.

4. To ensure that alarms, signals, and other methods of communication are in working order and effective, periodic tests of the system should be conducted without an actual evacuation. Prior notification regarding such tests should be provided to all occupants so that they will become familiar with the methods of notification.

7.7. EVACUATION PROCEDURES

A. Evacuation Procedures. Keeping in mind that the first consideration is life safety, the evacuation should be orderly and rapid.

1. Persons evacuating should not stop to take personal belongings with them (if this action in any way jeopardizes their safety), but should take purses/wallets, medicines, identification, and coats (during inclement weather) with them, if these items are readily accessible.

2. Doors and windows should be closed to provide effective smoke and fire containment, if the evacuation is due to a fire, but not locked in order to allow access to offices by emergency response personnel.

3. Individuals with special needs who require assistance should be identified in the planning process, and a plan must be developed and documented to address the needs of these individuals during an emergency. If internal safe rooms or areas of refuge are to be used, these areas must be coordinated in advance with local authorities and with special needs individuals. For additional guidance on developing plans for individuals with special needs, refer to Section 7.22.

4. Each office within an organization must have a system in place to account for its occupants once they have evacuated and/or relocated within the building as directed.

B. Evacuation Site and Reentry.

1. When a building or area is evacuated, the evacuees must know where to go. The choices of where evacuees should assemble are restricted by the configuration of the building, location of the building, facilities in the area, and the reason for evacuation.

2. For general building evacuation, a nearby park, an auditorium in a nearby building, etc., may be specified as an assembly area. The nature of the threat and/or intelligence may require use of an alternate assembly area.

3. It is important to set up a means of communicating to occupants when it is safe to reenter a building or to notify occupants that the building will have to remain closed for a period of time. The method of recalling occupants will often depend on where they have assembled. If the building has been cleared for reentry, a simple announcement made by the Emergency Operations Coordinator to the occupants may be sufficient, or each manager may be responsible for notifying his or her employees and visitors of reentry or closure. Whatever the chosen method, a plan should be in place and should be communicated to all occupants in advance of any emergency.

4. To ensure that personnel do not access unsafe areas or unsafe buildings, it may be appropriate to provide controls to ensure reentry does not occur into an unsafe area or building or to redirect occupants to an alternate reentry point of a building, especially if the emergency situation resulted in damage or obstructions.

5. Members of the facility's emergency organization will ensure that persons do not reenter evacuated areas until it has been determined safe to do so and only after the approval of the Designated Official. It is possible for persons visiting to be unaware that an area or building has been evacuated unless some means is established to indicate the area is unsafe and may not be entered.

7.8. SHELTER-IN-PLACE (SIP) PROCEDURES

A. Some emergency situations may require that the building NOT be evacuated. In cases of inclement weather (such as tornadoes or hurricanes) or in the event of the exterior release of a hazardous material, it may be safer to stay inside the building. In these cases, building occupants may be instructed to SIP, that is, remain in the building and congregate in corridors toward the interior of the building away from windows. During SIP scenarios, maintaining as much physical distance as possible from exterior openings such as doors and windows is important.

B. SIP procedures may specify going up or down levels in the building to provide the best possible protection and assembling at a specified alternate location.

C. SIP is a protective action that is voluntary (unless mandated by local law enforcement or public health authorities) to ensure public safety. Personnel will be permitted to leave the building when it has been determined it is safe to do so. A SIP action is taken inside the building with doors and windows closed to minimize the chance of injury (see Table 2 below) when one of the following emergencies occurs outside the building:

Table 2. SIP Action Considerations

ACTION CONSIDERATION	CONDITIONS
MOST LIKELY	Severe weather (tornado, hail, etc.)
	Civil unrest
	Accidental chemical release due to industrial or vehicle accident
LEAST LIKELY	Biological, chemical, or radiological attack

D. While it is anticipated that SIP will be of short duration, all occupants are encouraged to plan for unexpected, possibly longer contingencies and to maintain a personal supply of non-perishable food items in their working spaces. FEMA recommends that occupants consider having the following items available during any emergency.

1. Three-day supply of medicines. In the event the emergency lasts longer than expected or the occupant is unable to make it home to retrieve these items, a sufficient supply should be kept on hand. Occupants should ask their physician or pharmacist about storing prescription medications and ensure medications are stored safely and meet expiration dates and instructions on the label. It is also a good idea to have the name of the pharmacy or medication written down, just in case specialized medical care or assistance is required.
2. Small tote bag such as a fanny pack, backpack, etc. should be kept in close proximity to the occupant. This bag should be used to hold any emergency supplies.
3. Prepackaged emergency water. Water with a minimum two-year shelf life is recommended. One to two quarts should be sufficient for a short duration SIP

action lasting a few hours, but may not be sufficient for several days. If prepackaged water in pouches or boxes is considered, ensure it is protected from leakage because these packages may break while in storage.

4. Non-perishable, foil-wrapped foods, such as snack or high-protein bars that are light and easy to carry. An alternative is prepackaged bars with a five-year shelf life. These bars are high in calories and do not promote thirst. Use plastic bags or containers to reduce the risk of rodent and insect intrusion.
5. Small battery-operated (with extra batteries) or solar radio. The occupant may need to walk and not have any way of getting up-to-date information (extra batteries).
6. Small flashlight (with extra batteries). If possible, the occupant should purchase a radio and flashlight that use the same size batteries so they have to buy only one size and can use them interchangeably.
7. Two light/glow sticks to pin to clothes or carry in case the occupant has to walk in the dark.
8. Small multi-tool.
9. Two N95 paper masks. These masks are small, lightweight and inexpensive. They provide limited protection from dust.
10. A pair of vinyl latex gloves.
11. A pen and small notebook/telephone book. A book with telephone numbers, email addresses and emergency contact information of family, friends, neighbors, and medical personnel, etc., can be helpful to have during an emergency. While many people carry cell phones and electronic note pads, a hard copy backup is useful and would be helpful to medical personnel if the occupant needed medical attention.
12. Emergency rain poncho.
13. Emergency blanket.
14. Small first-aid kit.
15. Area map.
16. Cash, $50 in small denominations to buy food and gas in case the occupant is unable to use a credit card or debit cards. Occupants should keep all valuable items on their person at all times and not in their kit.

7.9. ACTIVE SHOOTER PROCEDURES

A. An active shooter is defined as an individual actively engaged in killing or attempting to kill people in a populated area. While the majority of incidents involve the use of firearms, for the purposes of this policy, the term "active shooter" may also apply to an individual armed with any other type of weapon (e.g., firearm, knife, explosives, etc.).

B. Active shooter situations are unpredictable and evolve quickly. In the event of an active shooter threat, it is DOC policy to employ the Department of Homeland

Security's "Run – Hide - Fight" strategy. Employees will decide the best course of action based on their training, observations and individual situations.

C. Upon the announcement of an active shooter situation, occupants and visitors will observe their individual situation and decide to Run, Hide, Fight and/or a combination of these individual response measures..

7.10. DRILLS

A. To be effective, an OEP must be tested. Rehearsing procedures assists the members of the emergency organization in becoming familiar with their duties and gives the occupants an opportunity to experience how an evacuation or SIP might occur.

B. A full-scale evacuation and a SIP drill will be conducted at least annually. DOC owned/leased facilities that are level 3, 4 or 5 are required to conduct one (1) of the following building exercises quarterly: Active Shooter, Evacuation, and Shelter in Place. The evacuation and SIP drills may be conducted as table top exercises provided a full scale evacuation and SIP drill occurred as required. It is recommend, but not required, that facilities that experience a high rate of occupant turnover or temporary personnel consider semi-annual exercises. In addition to the mandatory full scale annual exercises, facility managers can implement training drills without a total evacuation that consist of discussions about evacuation routes, duties and responsibilities of various occupants. These discussions should be followed by a walk-through of the evacuation routes. Drills of this nature can be conducted by groups or selected occupants periodically throughout the year.

C. Emergency Operations Coordinators will establish procedures to notify all appropriate authorities in the facility, such as the Designated Official, facility manager, and OEP Planning Team, prior to conducting a drill. Drills may be announced or unannounced. All drills will be followed by an assessment that includes after-action comments, observations, weaknesses or training deficiencies, and recommendations as determined by the drill results. Unannounced drills are more effective because they test actual emergency preparedness and provide the observers with stated objectives that will be tested.

D. The Designated Official/Emergency Operations Coordinator will maintain written records for all drills. These records will specify the date/time of the drill, scenario used, participants involved, actions taken by participants, and an after-action report, including any corrective action or improvements that are necessary.

7.11. ACTUAL EMERGENCY EVENTS OR FALSE ALARMS

A. Like drills, actual emergency events or false alarms that result in a SIP action and/or an evacuation of the building allow emergency management coordinators to test emergency plans and actions to be taken during a real emergency.

B. In order for an actual emergency event to be of training value to Emergency Operations Coordinators, each evacuation or SIP action must be followed by an assessment that

includes after-action comments, observations, weaknesses or training deficiencies, and recommendations as determined by the event.

C. The Designated Official/Emergency Operations Coordinator will maintain written records for all SIP actions and evacuations. These records will specify the emergency event, date/time of the event, participants involved, actions taken by participants, and an after-action report, including any corrective action or improvements recommended.

7.12. EMERGENCY RESPONSE ASSISTANCE

A. Medical Assistance. Medical assistance will not be required in all emergencies. However, the availability of medical assistance must be known in the event the emergency does result in injuries. In large facilities, planning must include provisions for obtaining medical assistance for events that result in large-scale injuries (see Section 7.23, Bomb Threat Checklist).

1. In the event of a medical emergency, professional medical assistance (rescue squad, fire department, etc.) must be called immediately. The first priority becomes aiding the injured persons after actions are taken to prevent further injuries. A quick response will decrease injuries. For this reason, occupants certified in first aid are an excellent resource. First-aid measures should not be relied on as final treatment but rendered only until professional medical assistance arrives.
2. To reduce response time as much as possible, the area surrounding the facility should be surveyed to identify resources of medical assistance that are readily available. Resources to be considered are:
   - Federal Protective Service (FPS) officers
   - Security force personnel
   - Health units
   - Police and fire department personnel
   - Rescue squads and hospitals
   - Local physicians
3. In most areas, 911 will activate a community emergency response; however, internal telephonic procedures, if in place, need to be documented and disseminated to all occupants.

B. Rescue.

1. Pre-planning will enhance the safety and chances of survival of those individuals who may be injured and/or trapped in a building or area. The larger the complex, the greater the possibility that an emergency will result in a situation that will require an organized rescue operation. Sources of assistance are normally local jurisdictional authorities. In any Departmental facility that has its own emergency service providers, the notification process must to be documented.
2. In those offices where natural disasters (tornadoes, earthquakes, etc.) may occur, an emergency pack containing items such as flashlight, first-aid kit, etc., may be

appropriate to keep on hand. The Emergency Operations Coordinator should check with the local FEMA office for advice.

C. Fire Emergency.

1. Fire is the most likely threat to life and property faced by Departmental facilities. Statistics show that fire continues to be a major cause of death, injury, property damage, and operational disruptions.
2. It is essential that security personnel work closely with safety personnel to create a comprehensive and coordinated effort to deal with the threat of fire. It is also important to coordinate support and responses with local fire officials.

D. Planning for Fire Emergencies.

1. All facilities with Departmental occupants will have written plans to manage fire emergencies. The plans should avoid unnecessary detail and complexity and must address all of the following actions:
   - Notifying the local fire department
   - Evacuating personnel
   - Directing the responding fire department to the scene of the fire and providing aid and information as necessary
   - Notifying facility management and respective agency management of the incident and extent of loss and damage
2. At a minimum, the appendix to the OEP for fire emergencies should include all of the following information:
   - Telephone numbers for the local fire department and appropriate officials in the occupant emergency organization
   - Location and proper use of fire alarms
   - Location and proper use of fire extinguishers
   - Evacuation procedures and routes
   - Procedure that identifies actions to assist individuals with special needs

E. Special Consideration for Information Processing Facilities.

1. Some facilities contain information technology (IT) processing equipment that is critical to the overall mission of the Department. Special consideration should be given to the protection of this equipment from fire and consequent smoke and water damage. Enhanced emergency response procedures for computer room personnel will be developed and included in the plan. IT systems personnel must be consulted on this part of the plan.
2. Minimum information regarding IT processing areas should include all of the following:
   - Evacuation routes
   - Location and criteria for use of emergency power cut-off switches

- Location and instructions for use of applicable fire extinguishers or other fire suppression systems and devices
- Storage location of roll of plastic or tarp to drape over IT equipment to protect it from water damage resulting from plumbing leaks or water from firefighting efforts

3. Electronic equipment that has been doused with water or other chemicals used in firefighting, or covered in smoke or soot, must be cleaned and/or dried as soon as possible to prevent permanent damage. The plan should include procedures for taking appropriate steps to clean contaminants from this equipment, followed by salvage procedures, as recommended by the manufacturer. IT systems personnel should develop this part of the plan.
4. Computer room emergency response procedures define what actions must be taken, assign responsibilities for each action, and provide necessary material and equipment in accessible locations. In some cases, there will be ample time to initiate loss control measures. In extreme emergencies, life safety will dictate immediate evacuation. For this reason, emergency response procedures will designate one or more individuals in each computer room who, in the event of an emergency, shall determine what can be done to protect equipment and records without endangering their lives or the lives of others.

7.13. BOMB THREATS

A. Bomb Threats. Each Departmental facility will have written plans to manage bomb threats and explosions. Although most bomb threats do not result in an explosion or discovery of an explosive device, it is very important that threats are thoroughly evaluated and that effective procedures exist for responding to threats.

1. Aside from explosion, the two significant dangers that exist with bomb threats are the sense of complacency that can develop from repeated hoax threats, and the panic that can result from a lack of appropriate action when a threat is perceived to be real. Both dangers can be partially overcome by instructing personnel in advance about the procedures involved in bomb threat reaction and by establishing a uniform bomb threat reporting procedure throughout the facility. Properly established reporting procedures will avoid information from being delayed or stopped on its way to the official with responsibility for evaluating threats.
2. Analysis of bomb threat data indicates that most threats are intended to create a sense of fear in the occupants and disrupt the facility. These outcomes can be avoided, to a great extent, by effective planning and organization.

B. Planning for Bomb Threats. An individual with a good general knowledge of the physical layout of the entire facility as well as the type of work that is done in each area needs to facilitate the planning process. This knowledge will help responders determine the areas where an explosive device could most easily be introduced and will facilitate quick and effective searches.

C. Bomb Search.

1. Depending on the facility, the FPS, local law enforcement units, or other federal law enforcement authorities may have primary search responsibility if a bomb is suspected in federal space. All Departmental occupants should be trained not to touch strange or suspicious objects or packages. Building occupants, because they are most familiar with their own office space, are expected to identify and report suspicious objects or packages located in their area to the appropriate security personnel, facility manager, or law enforcement authority. This action will expedite the identification, removal, and proper disposal of the suspected object. Under no circumstances should anyone attempt to move or examine a suspected explosive device.
2. When a bomb threat is considered to be serious, local and/or federal authorities trained in bomb search and disposal techniques will be called immediately to conduct the search. Searches should begin in the area(s) previously identified as most likely to conceal an explosive device unless a specific location was identified with the threat.
3. If a suspected explosive device is located, the Bomb Search Team with the federal and/or local authorities will recommend to the Designated Official whether a partial or full evacuation is necessary if the building has not already been fully or partially evacuation upon the initial bomb threat report.

D. Evacuation.

1. A decision to evacuate a facility when a bomb threat is received can only be made by an on-site Designated Official upon advice from the federal agency building manager and appropriate federal, state, and local law enforcement authorities. Even though most bomb threats are hoaxes, all factors of the threat must be considered. The safest course of action may appear to be evacuation. On the other hand, continued bomb threats, followed by automatic evacuation of the facility, could disrupt operations and encourage more threats. Some of the factors the Designated Official should consider in making a decision are:
   - Current trends involving bomb threats and explosions—the local police department may be a good source of information.
   - Character and consequence of recent threats in the area—percentage of threats that resulted in an explosion or an explosive device being found.
   - Recent activity of dissident groups, if any, that has been directed against government agencies, or specifically against the Department.
   - Characteristics of recent threats to local Departmental facilities, if any (security incident reports are one source of information).
   - Content of threat—whether the caller specified a location or time the bomb will explode.
   - Whether evacuation will place personnel in greater danger of injury than remaining in the building.

2. When there is doubt concerning a decision to evacuate, it is generally better to evacuate personnel because life safety is of primary importance.

7.14. HAZARDOUS MATERIALS

A. HAZMAT. HAZMAT is any substance or material that when released in sufficient quantities, poses a risk to health, safety, and property. HAZMAT includes chemical, radiological, or biological substances; materials such as water treatment chemicals, detergents, and other cleaning supplies; and explosives, radioactive materials, flammable liquids or solids, poisons, oxidizers, toxins, and corrosive materials. A HAZMAT incident may be a hazardous material spill or a threat of chemical or biological terrorism. Each facility must have a plan to address and manage hazardous material incidents.

B. Biological/Chemical Threat.

1. A biological threat may be an envelope or package purporting to contain a hazardous substance or a threat. Whatever the means of delivery, all Departmental facilities will have written plans that address actions to manage potential biological threats. It is essential that the Designated Official work closely with the FPS, if applicable, and local law enforcement and fire department authorities in developing a plan.

2. The plan will provide for notification of the Designated Official, the FPS (if applicable), and local authorities. As with any suspicious package, no attempt should be made to move the item or change the condition of the environment in any way. For example, do not place a blanket over the package or submerge a suspicious package in water, etc. Immediately isolate the hazardous area and areas that are in close proximity to the hazardous area to prevent entry by others.

3. Controlling contaminated areas, persons, etc. has a direct bearing on the decision to order a building evacuation, which, in turn, depends on the circumstances of the threat and where the danger is or is suspected to be. In most situations, a full evacuation will not be necessary. In many cases, a partial evacuation will be more advisable. In a partial evacuation, it is important that access to the hazardous area is controlled so that individuals do not inadvertently enter these areas.

C. Planning for HAZMAT Situations.

1. Emergency planners should check with the local fire department or HAZMAT response organization for assistance in reviewing and/or developing appropriate response procedures. Response procedures vary from one jurisdiction to another. Coordination with local emergency response organizations is essential.

2. The facility's Hazard Communications Program must include all of the following:
   - Identifying and labeling any hazardous material stored, handled, produced, and disposed of by the facility.
   - Obtaining Safety Data Sheets (SDS) for all hazardous material at the facility.

- Conducting HAZMAT training to ensure proper handling and storage of these materials.

3. Occupants must be trained to recognize and report HAZMAT spills and releases. The Designated Official must ensure the HAZMAT response plan includes all of the following:
   - Procedures for notifying management and local HAZMAT response organizations.
   - Procedures for warning occupants of incidents.
   - Procedures for evacuation.
4. Local emergency response organizations may be able to assist offices in training in-house response teams, organizing responses, and controlling HAZMAT incidents, if necessary, until local authorities arrive.

7.15. NATURAL DISASTERS

A. Natural Disasters. The most important time for mitigation planning is during facility site selection and determination of construction standards. Planning from the ground up is, however, rarely an option available to the facility manager. This, coupled with the current inability to prevent or accurately predict natural disasters, leaves emergency planners with the task of providing rapid, effective reactions to a realized threat.

B. Planning for Natural Disasters.

1. The first step in preparing for natural disasters is to identify the hazards. While this chapter does not provide specific direction for all hazards, the basic planning process can be adapted for any natural hazard. In this step, emergency planners will simply identify all of the threats/hazards that *might* affect or have affected their facility or other facilities in their general location, and then narrow the list to those threats and hazards that are most likely to occur. The plan must take an all-hazards approach.
2. Second, the hazards that have previously occurred or may occur should be listed in the plan with additional focus placed on these specific hazards. Information can be determined from the following sources:
   - Newspapers and other historical documents
   - Existing plans and reports
   - Experts in the local community, state, or region
3. Emergency planners should focus on the most prevalent hazard in their community. The local State Emergency Management Agency or EOC is an excellent starting point. Hazard websites are available to help in determining the probability that a specific hazard may affect the community. There are seven natural hazards that modern emergency planners consider prevalent; websites related to these hazards include:

Floods	Federal Emergency Management Agency (FEMA): http://www.fema.gov
Earthquakes	U.S. Geological Survey (USGS): http://www.usgs.gov

Tsunamis	National Oceanic and Atmospheric Administration (NOAA): http://www.noaa.gov
Tornadoes	FEMA: http://www.fema.gov
Coastal Storms	NOAA: http://www.noaa.gov
Landslides	USGS: http://www.usgs.gov
Wildfires	U.S. DHS/U.S. Fire Administration (DHS/USFA): http://www.usfa.fema.gov

4. Local weather services may also be contacted to obtain information about hazardous conditions most likely to occur in the area of a particular facility.

   Table 3 lists a Hazard/Threat Checklist that, although not comprehensive, may be used to assist each facility in identifying likely hazards and the probability level of each hazard to facility occupants. The first column lists the threats/hazards that could cause an emergency at the facility. (Note: These are threats that have or may potentially occur because of facility location or other physical, natural, or human factors.) Place checkmark in appropriate block to determine Hazard/Threat level where Low indicates Seldom or Potential occurrence, Medium indicates Infrequent occurrence, High indicates High occurrence and Critical indicates Frequent occurrence.

Table 3. Hazard/Threat Checklist

What are the threats/hazards that could cause an emergency at the facility? (NOTE: THESE ARE THREATS THAT HAVE OR MAY POTENTIALLY OCCUR, DUE TO FACILITY LOCATION OR OTHER PHYSICAL, NATURAL, OR HUMAN FACTORS)	LOW	MEDIUM	HIGH	CRITICAL
1. Active Shooter				
2. Arson				
3. Bomb Threat/Suspicious Package				
4. Civil Disturbance (Rioting)				
5. Communication Interruption				
6. Earthquake				
7. Electrical				
8. Explosion				
9. Fire (to include wildfires)				
10. Flood				
11. Hazardous Material Release (Chemical Biological Radiological Nuclear Explosive (CBRNE))				
12. Health Hazard/Disease				
13. Hurricane/Tornado/Windstorm				
14. Industrial Accident				
15. Internal/External Sabotage				
16. Mischief				
17. Network Disruption				
18. Power Failure/Interruption				
19. Severe Storm—Thunderstorm/Lightning				
20. Snow and Ice				
21. Strike				
22. Terrorism/Weapons of Mass Destruction				
23. Workplace Violence				
24. Vehicle (Close proximity of suspect vehicle to facility)				
25. Water Failure				
26. Temperature Extremes				
27. Tsunamis				
28. Improvised Explosive Device (IED) – Package/Vehicle				
29. Other (Identify)				

C. Office Closures.

1. Severe weather plans should include provisions for advising occupants of an office closing in the event that adverse conditions develop before regular business hours.

In large offices, use of local radio stations should be considered as a means of notification. In addition, some offices have set up toll-free numbers to use as notification of office closures.

2. All actions should be guided by the local servicing Office of Human Resource Management.

3. If local radio stations are used as a notification medium, the radio station call signs and frequencies will be included in the severe weather appendix of the OEP.

7.16. DEMONSTRATIONS AND/OR CIVIL DISTURBANCES

A. All Departmental facilities are subject to disruption that can result from civil demonstrations. Disruption can result when a demonstration is directed at the facility, when directed at other tenants of a facility occupied by the Department's organizational units, or when staged in areas adjacent to Departmental facilities.

B. All Departmental facilities will have written plans to deal with demonstrations. The emphasis on planning for demonstration responses must be on minimizing the potential for confrontation that can develop into violence and for avoiding the involvement of Departmental occupants with demonstrators or reporters.

C. Departmental occupants should be instructed to continue working and to stay away from windows and doors to the extent possible during demonstrations. Local law enforcement agencies and the FPS (if applicable) should be contacted in order to develop coordinated plans to handle demonstrations.

7.17. WORKPLACE VIOLENCE

While not identified by GSA as a requirement of an OEP, a plan to address workplace violence is strongly recommended. According to the Department of Labor (DOL), violent acts rank among the top three causes of workplace fatalities for all workers. Facility managers should consider putting together a team of trained personnel from within the organization, including supervisors, security personnel, human resource personnel (e.g., Safety, Employee Relations, and Employee Assistance Program Counselor, etc.) to respond to and diffuse potential or real threats of workplace violence.

7.18. HOSTAGE SITUATIONS

A. Hostage Situations. When dealing with hostage incidents, in an ideal setting, properly trained and equipped law enforcement agencies are available to control these situations. However, because of the wide range of Departmental locations, ideal conditions are not always attainable, especially in the early development of an incident.

B. Planning for Hostage Situations. All Departmental facilities will have plans to manage hostage situations that are coordinated with appropriate law enforcement agencies. The plan will include, at a minimum, telephone numbers for law enforcement agencies that are able to provide support in a hostage situation.

C. **Guidelines.** The following guidelines are provided as general background on the control of hostage situations and will be used until the appropriate law enforcement agency or agencies take control of the incident, are able to isolate the area by evacuating occupants from the site, and are able to cordon off the area to prevent entry by unauthorized persons.

a) Until law enforcement personnel arrive and take control of the situation, communications with hostage captors should be maintained by personnel designated by the Senior Departmental Official/Designated Official who will record any communications from the hostages/takers and provide the information to the responding law enforcement personnel. Under no circumstances will communications include any attempts by untrained personnel to negotiate.

b) Other federal law enforcement agencies and local police departments will be contacted to determine the resources available for handling hostage incidents. Assistance with and training for hostage situations should be pursued with local and state or federal law enforcement agencies.

7.19. REPORTING SUSPICIOUS ACTIVITIES

The Senior Departmental Official, Emergency Operations Coordinator or Designated Official should establish written procedures for occupants in a facility to report any suspicious persons or activities, unlawful acts, or other incidents requiring a response. This report should be provided to the SSO, nearest FPS office (if applicable), or local law enforcement authority, as appropriate. The following are a few tips to guide occupants in keeping their area and property secure:

- Lock offices when left unoccupied.
- Secure all property, both personal and government.
- Wear government-issued identification at all times while in the facility.
- Challenge those individuals without a visible badge or locate someone with the authority to challenge them (such as building guards).
- Report any suspicious activity immediately to the appropriate security or emergency coordination official.

7.20. EMERGENCY COMMUNICATION SYSTEM

A. Emergency plans require rapid communication in order to be effective. Notification of emergency situations to occupants in a facility should be accomplished via an Emergency Broadcast System, by use of a public address (PA) system, or through a combination of communication devices and IT networks. Emergency alerts should communicate the appropriate information to occupants without unnecessarily tying up the communication systems itself.

B. In addition to current systems available for emergency communications, a pyramid or cascade system is a secondary means of effectively alerting organizational personnel during an emergency.

1. The concept of the cascade or telephone tree call system is simple. One individual initiates the system by calling one set of individuals, which then calls another set of individuals. The number of calls for which each individual is responsible vary with

the size of the organization, but the number of persons contacted should be as few as possible.

2. For OEP purposes, the individual responsible for initiating the cascade call systems should be the Designated Official or Departmental official responsible for initiating emergency action.

3. Any communication system that contains incorrect names and telephone numbers is useless; therefore, reviews are necessary to validate the system's effectiveness. Whatever method of communication is used to initiate emergency action plans, the system should be validated quarterly or more frequently, if necessary.

C. Total reliance on the telephone or other systems that do not have backup or self-contained power sources as the sole means of communication should be avoided during emergencies. Because the results of a serious emergency condition frequently include downed power and telephone lines, alternate communication systems should be devised. Alternate communications systems that should be considered are radios using batteries or backup power sources, beepers, cellular telephones, or messengers.

Table 4. Occupant Emergency Plan Development Guidelines Checklist

TOPIC	STATUS/ CONTACT	DATE COMPLETED
I. Form the OEP planning team—To develop an effective OEP, the team should include representatives from safety, security, environmental, facilities, engineering, maintenance, IT, human resources, and as appropriate, legal offices. The OEP team can be formal or informal, or it can be part of an existing team such as a risk assessment team. Assigning a facility liaison from local fire and police departments, etc., is helpful. The size and make-up of the team depends on the complexity of the facility's operations. A. Establish authority to show that the senior leadership supports the planning team in the development of the OEP. B. Create a mission statement. 1. Defines the purpose of the plan. 2. Involves the entire organization. 3. Defines the authority and structure of the planning group. C. Establish a schedule and budget if appropriate. D. Develop the OEP. 1. GSA OEP templates can be found on the GSA Emergency Management and Security website at http://www.gsa.gov/graphics/pbs/OEP_Guide_Supplement_3_template_11_16_07.pdf. 2. Guidance on occupants with special needs can be found on the Department of Labor (DOL) website at http://www.dol.gov/odep/topics/EmergencyPreparedness.htm		
II. Analyze the facility's capabilities. A. Review current internal documents to determine the facility's preparedness, i.e., evacuation and/or fire plan, safety and health program, environmental policies, security procedures, facility closure policy, hazardous materials plan, etc. 1. Does the current OEP address common risks (e.g., fire, medical, and severe weather) as well as any unusual risks that may threaten the organization (e.g., earthquakes, tsunamis, or CBRNE incidents)?		
2. Does the current OEP include evacuation and SIP procedures as a response to emergencies?		
3. Has a command or operations center been established?		

TOPIC	STATUS/ CONTACT	DATE COMPLETED
4. Has an alerting system been established to inform occupants and members of the emergency organization that an emergency has occurred?		
5. Does the alerting system notification distinguish among the various types of emergencies? Are occupants familiar with the procedures for initiating alarms?		
6. Are emergency procedures as simple as possible so they can be implemented rapidly and with minimum confusion in stressful situations?		
7. Are emergency telephone numbers posted in the command center and throughout the facility? Are they published in the facility telephone directory? Are they reviewed and updated frequently?		
8. Are all applicable persons aware of the procedures for reporting fires, medical emergencies, hazardous material releases, unlawful acts, and other reasonably foreseeable emergencies?		
9. Is there a procedure for alerting all applicable persons when severe weather is forecast or imminent?		
10. Are evacuation procedures and emergency assembly areas away from the building identified and familiar to all applicable persons? Are there nearby as well as remote assembly areas to accommodate both minor and catastrophic emergencies?		
11. Have SIP procedures been implemented and communicated to all applicable persons?		
12. Have special procedures for evacuating and SIP been established for persons with special needs?		
13. Have Lockdown procedures been implemented and are building occupants aware of actions they need to take if a lockdown event occurs?		

TOPIC	STATUS/ CONTACT	DATE COMPLETED
14. Has special attention been given to the unique emergency requirements of facility childcare centers? Note: Childcare center plans should be incorporated into the facility's plan, although development of this plan is the responsibility of the agency that provides direct oversight of the center.		
15. Meet with external groups to learn about the resources available, i.e., community emergency management offices, Local Emergency Planning Committees (LEPC), mayors or community administrators, fire and police departments, utility companies, etc.		
B. Identify applicable codes and regulations, such as: 1. Occupational Safety and Health 2. Environmental 3. Fire		
C. Identify the facility's critical assets and essential functions		
D. Identify internal resources and capabilities 1. Personnel 2. Equipment 3. Facilities 4. Backup systems—communications, information systems support, emergency power, etc. 5. Other resources and capabilities		
III. Identify the types of emergencies that could occur and assess how likely each is to occur.		
A. Fire.		
B. Severe weather (hurricane, flood, tornado, earthquake, etc.) **Tools**—FEMA's severe weather hazards website at www.fema.gov		
C. Civil disturbance		
D. Bomb/bomb threat		
E. Hazardous materials spill— Chemical, Biological, Radiological, Nuclear Explosive		
F. Active Shooter		

TOPIC	STATUS/ CONTACT	DATE COMPLETED
IV. Assess the impact of potential emergencies on the organization's ability to achieve its mission and the impact on its personnel and assets. Once the types of emergencies that could occur have been identified and the likelihood of their occurrence has been assessed, determine what impact each of the emergencies would have on the organization's: 1. Ability to perform its mission 2. Departmental personnel and other Departmental facility occupants 3. Assets		
V. Conduct a risk assessment of the facility. A. How secure are the buildings/structures? Risk assessments include an examination of the criticality, threat, and vulnerability of the facility. The risk assessment is a service provided by the facility's SSO.		
B. How could CBRNE elements enter the buildings/facilities? **Tool**—Environmental Protection Agency (EPA) document provides checklists to create a building air quality profile. Reference the EPA website at www.epa.gov.		
C. What actions could be taken to "strengthen" the buildings/facilities? **Tool**—National Institute of Safety and Health's (NIOSH) Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks, May 2002. Reference the NIOSH website at www.cdc.gov/niosh.		
VI. Determine what types of personal emergency planning actions are being performed by occupants. Have occupants assembled their own personal disaster supply kit for the office? **Tool**—FEMA's booklet "*Are You Ready?*" provides recommendations. Reference the FEMA website at www.fema.gov.		
VII. Create the OEP Development Working Group. Composed of subject matter experts—Remember that these experts assist in the development of the plan but may not end up on the OEP Team. Personnel may include safety, security, facility, emergency planners, industrial hygienist, medical personnel, etc.		
VIII. Develop the OEP. A. The OEP protects all occupants, assets, and the facility's mission capability. The results of the hazard identification and risk assessments generally determine the complexity of		

TOPIC	STATUS/ CONTACT	DATE COMPLETED
the OEP.		
B. The following items are some topics to consider for inclusion in the OEP:		
1. Introduction, purpose, and scope of the OEP. **Tool**—FEMA—A comprehensive document to assist in developing the OEP as well as the overall Emergency Plan, conducting risk assessments, etc. Reference the FEMA website at www.fema.gov.		
2. Document building and tenant information.		
3. Identify the building emergency organization. **Note**—Include contacts, titles, and telephone numbers in a master list; outline roles and responsibilities; and identify a facility command center for the emergency organization's use.		
IX. Reference Federal Regulations and Authorities. A. Once the OEP Development Working Group is assembled, it should review and include references and information to the following regulations and authorities in the OEP, as appropriate: 1. DHS OEP Guide with Supplements 1, 2, and 3. 2. 41 FMR 102.80 Safety and Environmental Management—reference the GSA website at www.gsa.gov. 3. 29 CFR 1910.38 Emergency Action Plans—reference Occupational Safety and Health Administration (OSHA) website at www.osha.gov.		
4. U.S. Department of Commerce Manual of Security Policies and Procedures. 5. Departmental Organization Orders (DOOs) 6. Departmental Administrative Orders (DAOs)		
B. The following scenarios must be addressed in the OEP: Evacuation Procedures— 1. Escape routes 2. Evacuation diagrams 3. Designated meeting areas		

TOPIC	STATUS/ CONTACT	DATE COMPLETED
4. Evacuation of persons with special needs 5. Evacuation chairs 6. Pre-arranged staging areas **Tool**—"The Emergency Preparedness Initiative—Guide on the Special Needs of People with Disabilities for Emergency Managers"—Reference the DOL website at www.dol.gov. C. Procedures to Document Evacuated Occupants: **Tool**—OSHA's Evacuation Plan E-Tool—Reference the OSHA website at www.osha.gov. OSHA Evacuation Planning Matrix—Reference the OSHA website at www.osha.gov. National Fire Protection Association (NFPA) Fact Sheet —Download the Fact Sheet and go to excerpts from Chapter 6—Emergency Evacuation Drills. Reference the NFPA website at www.nfpa.org.		
D. SIP Procedures. 1. Identify interior meeting areas and their space and protection capacity. 2. Establish working areas for senior staff to continue mission-critical operations. 3. Establish procedures for— a. Assembling of personnel b. Accountability of personnel c. Addressing medical/physical needs 4. Establish procedures for shutting down mechanical and ventilation equipment **Tool**—SIP at your office by National Institute for Chemical Studies (NICS)—Reference the NICS website at www.nicsinfo.org OSHA Evacuation E-Tools, SIP—Reference the OSHA website at www.osha.gov		
E. Active Shooter Procedures 1. Describe the actions to take when confronted with an active shooter and to assist responding law enforcement officials; 2. Recognize potential workplace violence indicators; 3. Describe actions to take to prevent and prepare for potential active shooter incidents; and 4. Describe how to manage the consequences of an		

TOPIC	STATUS/ CONTACT	DATE COMPLETED
active shooter incident. a) Run **If there is an accessible escape path, attempt to evacuate the premises** b) Hide **If evacuation is not possible, find a place to hide where the active shooter is less likely to find you** c) Fight **As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter** Reference to DHS website at www.dhs.gov/active-shooter-preparedness		
F. Available emergency services and how to obtain them.		
G. Hazard Mitigation Procedures (actions taken to reduce the impact of identified hazards). **Tools**—Guidance for Protecting Buildings from Airborne CBRNE Attacks—Reference the OSHA website at www.osha.gov. **Tools**—Basic Strategies for Building Protection—Reference the U.S. Army website at www.army.mil.		
H. Emergency Procedures—Reference the FEMA website at www.fema.gov. 1. Fire emergencies 2. Medical emergencies 3. Severe weather a. Hurricane b. Flood c. Tornado 4. Earthquake 5. Civil disturbance 6 Bomb/bomb threats 7. Hazardous material: chemical, biological, or radiological 8. Workplace violence and hostage situations. 9. Unlawful acts		

TOPIC	STATUS/ CONTACT	DATE COMPLETED
I. Communications. 1. Warning systems 2. Communications during emergencies 3. Public address system—Use pre-recorded emergency messages 4. Radios and emergency telephones—Ensure they can communicate with each other 5. Special circumstances—Communicating with the deaf and hard of hearing **Tool**—NFPA Fact Sheets—Fire Safety for the Deaf and Hard of Hearing—Reference the NFPA website at www.nfpa.org 6. Communicating with occupants a. Establish organizations/divisions/etc., telephone trees to notify occupants after hours b. Establish a call-in number so occupants away from the office can get information		
J. Training 1. OEP Team Tools a. Office of Personnel Management (OPM) Manager's Guide to Emergencies—Reference the OPM website at www.opm.gov. b. FEMA—"Are You Ready?" booklet—Guide to all types of disasters and disaster supply kit recommendations. Reference the FEMA website at www.fema.gov. 2. Tools a. Agency Employee's Response to Emergencies Guide Template—This guide outlines what occupants should do in the event of an emergency. The template should be tailored to the facility's specific emergency procedures. Once the guide is tailored to each facility, it should be included in new employee orientations. b. DHS—"Preparing Makes Sense. Get Ready Now" brochure—Reference the DHS website at www.dhs.gov. c. OPM's "Employee Guide to Emergencies"—Reference the OPM website at www.opm.gov. d. OPM's "Family Preparedness Guide"—Reference		

TOPIC	STATUS/ CONTACT	DATE COMPLETED
the OPM website at www.opm.gov.		
K. Drills—The intent of emergency readiness drills is to ensure that unit personnel are aware of their responsibilities, as outlined in the OEP, in the event of an emergency. Drills are also intended to ensure occupants are familiar with established procedures. 1. Red Cross SIP Guidance—Reference the Red Cross website at www.redcross.org. 2. NFPA—Developing a Fire Plan and Conducting Fire Drills—Reference the NFPA website at www.nfpa.gov. 3. Test and evaluate the OEP by conducting drills and testing equipment. Drills and testing should be documented.		
L. Evaluations and corrective action.		
M. Implement the OEP and coordinate with local responders.		
N. Train OEP participants/responders and occupants.		
O. Update the OEP annually, or more frequently as changes occur.		

7.21. OCCUPANT EMERGENCY PLAN (ABBREVIATED) GSA FORM 3415

(This form is provided as a suggested guide for storefront and/or ground level small office space)

AGENCY	ADDRESS	DATE

NAMES AND TELEPHONE NUMBERS OF EMERGENCY CONTACTS

NAME/TITLE	OFFICE PHONE	OTHER PHONE
Fire Department		
Police Department		
Medical Assistance		
Federal Protective Service		
Building Manager/Lessor		
Official-in-Charge		
Bomb Squad		

EMERGENCY ORGANIZATION INFORMATION

(Coordinator, Monitors, and Bomb Search Officer)

	NAME	DUTY	OFFICE PHONE	OTHER PHONE
1.				
2.				
3.				

EMERGENCY PLAN GUIDANCE

IMPORTANT! Know Evacuation Routes. Know the Plan of Action. Be prepared to assist persons with special needs.
Bomb Threat Checklist on Reverse Side

	FIRE OR SMOKE		BOMB THREAT
	Sound building alarm		Complete information on the back of this form
	Call fire department		Notify Official-in-charge
	Notify Official-in-charge		Notify police
	Notify building manager/Lessor		Notify building manager/Lessor
	Notify Federal Protective Service		Notify Federal Protective Services
	Assist fire department		Search immediate area and public areas for any suspicious packages or objects
	Evacuate area immediately		
	Close windows and doors (do not lock)	If suspicious package or bomb is found:	
	HAZARDOUS MATERIALS		Do not touch
			Notify bomb squad
	Do not handle the substance		Evacuate the area
	Do not clean the substance		SEVERE WEATHER
	Isolate employees		
	Keep employees calm		Secure objects outside building
	Notify Federal Protective Service		Prepare to move to place of safety
	Notify fire department		Stay away from large windows
	Shut off the HVAC		For tornado, open windows
	CIVIL DISTURBANCES		Know location of utility shutoff valves and switches
			Stay tuned to weather reports
	Notify Official-in-charge		Standby for further instructions
	Secure all doors		EARTHQUAKE
	Notify police		
	Notify building manager/Lessor		Take cover under table, desk, or in a doorway
	Notify Federal Protective Service		Do not run outdoors

7.22. EMERGENCY PROCEDURES FOR PERSONS WITH SPECIAL NEEDS

In compliance with the Americans with Disabilities Act (ADA) and the Rehabilitation Act of 1973, as amended, the Department has established guidelines for persons with special needs requiring temporary or permanent assistance (e.g., expectant mothers, and those who are hearing impaired, sight impaired, mobility impaired, have heart conditions, or who have injured or broken limbs, etc.).

Before special accommodations can be made, persons needing them must be identified. A list of individuals needing assistance should be current and included in the facility's OEP. This list should be accessible by the emergency personnel to assist in the emergency evacuation. However, it should be understood that there are many individuals who are protective of their right to independence and privacy and who may be reluctant to have their names put on this list. Some disability categories are easily recognizable, and in these cases, the individual can be approached to ask what can be done to assist them during an emergency. Another option that may be considered to assist persons with special needs is to ensure that each person has an Individual Emergency Plan (IEP). An IEP is a detailed plan for Departmental occupants who are voluntarily self-identified as needing assistance during an emergency.

Trained volunteer emergency buddy systems are widely accepted as a way to assist persons with special needs during an evacuation or SIP event. In the event of an emergency, the primary means of providing assistance to special needs individuals will be their identified emergency "buddies." If an occupant believes that he or she does not require assistance, the Rehabilitation

Act of 1973, as amended, generally prohibits an employer from requiring that an occupant or visitor with a disability accept a reasonable accommodation. In some cases, there will be someone who will need some special assistance in the event of a fire or other emergency requiring evacuation. Identifying these individuals in advance and knowing their locations is essential.

Do not lose sight of the fact that some persons with special needs may not recognize their own need for assistance. In addition, allowances for visitors present in the building should also be made. The importance of identifying persons with special needs should be shared during the orientation process because conditions change and persons can become temporarily disabled and require assistance.

For those with respiratory disorders, such as asthma or emphysema, the onset of symptoms can be triggered by stress, exertion, or exposure to small amounts of dust or smoke. Plans should cover a reminder that those individuals bring inhalation medication before leaving the workplace. Persons with cardiac conditions should be reminded to take their medications. A "buddy" should plan to offer them assistance in walking because they may have reduced stamina and require frequent rest periods.

The standards of the Americans with Disabilities Act (ADA), which apply to the Rehabilitation Act, require employers to keep medical information about individuals with disabilities confidential. These provisions, however, include an exception that allows an employer to share medical information with first-aid and safety personnel. This exception would allow an employer to share information about the type of assistance an individual needs in the event of an evacuation with medical professionals, emergency coordinators, floor monitors, colleagues who have volunteered to act as buddies, building security officers who need to confirm that everyone has been safely evacuated, and other non-medical personnel who are responsible for ensuring safe evacuation. These individuals are entitled to the information necessary to fulfill their responsibilities under the employer's OEP.

A. Areas of Refuge/Rescue Assistance.

1. Areas of refuge (close to exits) should be considered and identified for persons with special needs. There is always a possibility that the sprinkler system will fail to extinguish the fire, resulting in a problem with smoke propagation. It is quite possible for a person with a special need to be stranded and overcome with smoke before the arrival of the rescue personnel, given the difficulty in locating someone in a smoke-filled building. To address these possibilities, contingency plans are needed for providing safety to these individuals while they await assistance from fire department personnel or other individuals providing rescue.

B. Emergency Buddy Duties.

1. Each special needs individual should have assigned at least two buddies who are work associates of the special needs individual.
2. An individual with a permanent or major impairment generally knows the best way to be assisted. Buddies providing assistance should be trained in how to help without causing injury to themselves or others. This is especially relevant if someone needs to

be lifted or carried. To be effective, the person and the buddy must be able to make contact with each other quickly. Practice sessions (in advance) need to be conducted to ensure that buddies are capable of handling their assigned tasks and that there is a level of comfort from the individual being assisted.

3. Buddies should plan to:
   a. Be involved in the development of the IEP (if this is in place), including planning and training of the person with special needs.
   b. Upon notification of an emergency, report to the person with special needs and follow that individual's IEP.

C. The formulation of an IEP consists of the following steps:

1. Start the process after the individuals with special needs or temporary/permanent medical restrictions report that they will need assistance. This step requires that these individuals report their need for assistance to the applicable Human Resource Management's Office of Occupational Safety and Health for the facility where the individual is located.
2. Schedule a one-on-one meeting to evaluate the extent of the individual's limitations, determine the need for specialized evacuation equipment (e.g., evacuation chairs, wheelchairs, etc.) and/or procedures, establish an alternative evacuation route and/or method; and outline individual emergency procedures.
3. Recruit a minimum of two emergency buddies from the appropriate office and/or operating unit and train them. This training will include the individual requesting assistance, the supervisor, and the buddies. Exercise this training plan with the buddies until their response and the level of comfort of the individual with special needs is second nature.
4. Develop interim emergency procedures prior to finalizing the written IEP.
5. Schedule regular training for designated emergency buddies.

   NOTE: Persons with special needs should notify the Office of Occupational Safety and Health (OSHA) whenever their IEP needs to be updated or revised because of changes in emergency buddies, the healing of the temporary disability, etc.

D. Special Equipment Considerations.

1. Hearing Impairment.
   Signaling devices, strobe lights, and vibratory pagers are designed to alert persons through use of light, vibrations, and air movement (systems used for emergency notification must comply with UL1971, the Underwriter Laboratories *Standard for Emergency Devices for Hearing Impaired).*
2. Vision Impairment.
   a. Braille signs to mark egress doors.
   b. Audible directional instructions (transmitted by low power radio waves or infrared beams, which act as signals when one approaches a stairway).

c. Exit signs that flash and sound internal horns when activated by the building fire alarm system.

3. Movement Impairment.
   a. Portable, controlled descent chairs (an individual transfers from the wheelchair to this descent chair for stairwell evacuation) and is aided by an individual trained to properly use this device.

   b. For more information on specialized escape devices, refer to "*Egress Procedures & Technologies for People with Disabilities.*" Reference the DOL website at **www.dol.gov.**

E. Following an Evacuation.

1. Ensure that after exiting the building, individuals with special needs are not abandoned but are led to a place of safety (designated assembly area or other safe location if assembly area is not accessible) and that a colleague(s) remains with them until the emergency is over. Consider inclement weather and the unique needs of the individual during this time. If assisting a hearing-impaired person, offer pencil and paper if you are unable to understand the individual's speech or hand gestures as visual cues. Do not leave any special needs individual unattended or without needed assistance following an emergency.

7.23. BOMB THREAT CHECKLIST

Table 8 Bomb Threat Checklist

BOMB THREAT CALL PROCEDURES

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist (reverse side) immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of the call, do not hang up, but from a different phone, contact FPS immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by email:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

DO NOT:

- Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
- Evacuate the building until police arrive and evaluate the threat.
- Activate the fire alarm.
- Touch or move a suspicious package.

WHO TO CONTACT (select one)

- Follow your local guidelines
- Federal Protective Service (FPS) Police
  1-877-4-FPS-411 (1-877-437-7411)
- 911

BOMB THREAT CHECKLIST

Date: _____ **Time:** _____

Time Caller Hung Up: _____ **Phone Number Where Call Received:** _____

Ask Caller:

- Where is the bomb located? (Building, Floor, Room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact Words of Threat:

Information About Caller:

- Where is the caller located? (Background and level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Caller's Voice

- ☐ Accent
- ☐ Angry
- ☐ Calm
- ☐ Clearing throat
- ☐ Coughing
- ☐ Cracking voice
- ☐ Crying
- ☐ Deep
- ☐ Deep breathing
- ☐ Disguised
- ☐ Distinct
- ☐ Excited
- ☐ Female
- ☐ Laughter
- ☐ Lisp
- ☐ Loud
- ☐ Male
- ☐ Nasal
- ☐ Normal
- ☐ Ragged
- ☐ Rapid
- ☐ Raspy
- ☐ Slow
- ☐ Slurred
- ☐ Soft
- ☐ Stutter

Background Sounds:

- ☐ Animal Noises
- ☐ House Noises
- ☐ Kitchen Noises
- ☐ Street Noises
- ☐ Booth
- ☐ PA system
- ☐ Conversation
- ☐ Music
- ☐ Motor
- ☐ Clear
- ☐ Static
- ☐ Office machinery
- ☐ Factory machinery
- ☐ Local
- ☐ Long distance

Other Information:

_____

_____

Threat Language:

- ☐ Incoherent
- ☐ Message read
- ☐ Taped
- ☐ Irrational
- ☐ Profane
- ☐ Well-spoken

_____

_____

_____

Homeland Security

establishing, and maintaining a Departmental Occupant Emergency Program for organizational units in the Department. The Director will carry out this responsibility by providing standards, guidelines, and procedures for development of comprehensive OEPs that protect all Departmental occupants and workspaces. In addition, the Director will develop a program to evaluate the OEPs in the respective operating units.

C. **Heads of Operating Units.** The head of each operating unit is responsible for ensuring the safety and security of all personnel in the operating unit. This includes the development and implementation of OEPs for each facility assigned to his or her respective unit and ensuring that development of the OEP is coordinated with the Office of Security (OSY) headquarters as well as the GSA (or other lessor) in facilities administered by another organization. A representative (i.e., Safety Officer or Director of Facilities) of each operating unit head must be delegated the authority to review the OEP for each facility under that head's purview on an annual basis to **endorse the adequacy of the OEP and training.**

D. **Facility Manager.** Each facility manager is responsible for ensuring that OEPs are developed, coordinated, and implemented to protect the personnel, property, and information at the Departmental facility they administer or support.

E. **Designated Official.** The Designated Official in each facility is responsible for coordinating development, implementation, and maintenance of the OEP of his or her site. At those facilities where the Department is the primary federal agency, the highest ranking official at the facility, or alternatively, a designee selected by mutual agreement of occupant agency officials, will serve as the Designated Official and will be responsible for coordinating development, implementation, and maintenance of the OEP. At those facilities where the Designated Official is not a Department employee, the senior Department official at that site will work with the facility's Designated Official to develop, implement, and maintain the plan. The Department's senior-level official should be an employee with sufficient knowledge to carry out the requirements of this position. This position may be delegated in writing, and the person holding the position shall retain oversight of the OEP for all Department occupants.

F. **Managers and Supervisors.** All managers and supervisors are responsible for cooperating with the Designated Official to implement and maintain an OEP for the facility. Managers and supervisors who have employees assigned as Emergency Response Team (ERT) members supporting the OEP will notify the Designated Official when any team member transfers, retires, or because of extraordinary work and/or circumstances, can no longer perform his or her duties as an ERT member. The manager or supervisor may identify a replacement member and notify the Designated Official of this change. The manager or supervisor will also ensure that all occupants are aware of and comply with the guidance contained in the facility's OEP.

G. **Emergency Response Team Members.** The ERT is composed of trained personnel, established to assist occupants and to perform important functions in the event of an

Chapter 8. Foreign Travel

8.1. Travel Security

The Office of Security (OSY) shall interpret and monitor compliance with security-related policies, standards, criteria, and instructions incorporated in the Department of Commerce Travel Handbook (CTH) and shall approve requests for exceptions to security requirements related to foreign travel. Each operating unit's Foreign Travel Coordinator is responsible for assuring that any CTH security requirements are met.

8.2. Conduct and Reporting Requirements

A. Travelers on official foreign travel will be subject to the rules, regulations, and guidelines established by the Embassy or Foreign Service post in the country they are visiting, including pre-travel country-specific counterintelligence briefings.

B. All employees are required to report all unusual or suspicious contacts they have with individuals from foreign countries to the U.S. Embassy Regional Security Officer and OSY Investigations and Intelligence Division (IID) through their Servicing Security Office. Specifically, any contact with a foreign national either within or outside the scope of official activities must be reported when:

1. Illegal or unauthorized access to classified or sensitive information including Export Administration Regulations controlled technology, International Traffic in Arms Regulation technology, personally-identifiable information, proprietary or not-for-public release data, procurement sensitive information, Classified National Security Information, and Controlled Unclassified Information is sought.
2. The employee is concerned he or she may be the target of an actual or attempted exploitation by a foreign entity.
3. Any suspicious or noteworthy incidents occur involving a foreign national.

C. Departmental employees granted access to Sensitive Compartmented Information shall report all foreign travel to OSY Counterespionage Division (CED), who will make notification to OSY IID and the Central Intelligence Agency. Departmental employees may report such foreign travel through their unit's SSO who will ensure CED is provided immediate notification.

8.3. Briefing and Debriefing

A. Travel briefings are required on an annual basis for employees traveling on official business to locations abroad.

1. The Foreign Travel Briefing (FTB) program is coordinated by OSY Anti-terrorism Division (ATD). ATD can be contacted at (202) 482-2942 or OSYOC1@doc.gov.

2. DOC travelers who receive country clearance will be reminded by OSY they must have completed the FTB within the past year. The FTB is accessible through the Commerce Learning Center site.
3. Certain country-specific counterintelligence briefings are consolidated within the FTB. If required by the U.S. Embassy, additional country-specific briefings can be arranged through OSY.
4. Senior officials at the Herbert C. Hoover Building may request a desk-side briefing by contacting OSY ATD.

B. Debriefings may be conducted by OSY IID agents or SSOs with approval from and review by the IID on a case-by-case basis or in instances where DOC personnel travel to a foreign country for 90 days or longer.

SECTION II PERSONNEL SECURITY

Chapter 9. Personnel Security Policies

9.1. PURPOSE

The Manual of Security Policies and Procedures (the Manual) implements the policies and procedures that govern the management and administration of the security programs in the Department of Commerce (Department). Section II of the Manual prescribes the policies, procedures, and standards that govern the granting of eligibility for access to classified National Security Information (NSI); the procedures required to process security and suitability investigations; the adjudication criteria for determining eligibility for access to NSI; the conditions that may result in the suspension, revocation, downgrade, or denial of an individual's eligibility for access to NSI; and the requirements for allowing an individual access to special classified programs.

9.2. APPLICATION

A. Security and suitability investigations provide an assessment of an individual's potential likelihood to promote the efficiency and integrity of the Department's operations when filling a particular position. These investigations are also used to determine whether employment or retention in employment is consistent with the national security. The Personnel Security Program ensures that all personnel working within the Department are suitable for employment and are trustworthy.

B. The policies, procedures, and standards prescribed in this section apply to the employment of employees and applicants in the Department, as well as contractors, guest researchers, committee members, students and trainees, and other persons designated by the Secretary of Commerce to have access to NSI. In addition, senior managers, supervisors, and employees are responsible for familiarization and compliance with all personnel security regulations and procedures.

C. Questions concerning personnel security policies should be referred to the Servicing Security Officer. The OSY's Assistant Director for Counterespionage shall provide the Department's interpretation of security policy or procedures and, as necessary, provide written guidance to heads of operating units or Departmental offices. Policy or procedural questions concerning suitability should be referred to the Servicing Human Resources Management Office.

D. The Assistant Director for Counterespionage shall review adverse information relevant to an individual's access to NSI and may suspend, restrict, downgrade, propose denial, or propose revocation to an individual's access to NSI in accordance with the policies and procedures of the Manual.

E. Individuals will be appointed to a position in the Department only in accordance with the investigative requirements for suitability prescribed in the Office of Personnel

Management (OPM) Suitability Processing Handbook and the investigative requirements for access to NSI provided in this manual.

F. Questions concerning personnel security policies should be referred to the Servicing Security Office (SSO). The OSY Assistant Director for Counterespionage shall provide the Department's interpretation of security policy or procedures and, as necessary, provide written guidance to heads of operating units or Departmental offices. Policy or procedural questions concerning suitability should be referred to Servicing Human Resources Office.

9.3. PERSONNEL SECURITY POLICIES

Policies pertaining to the Department's personnel security program are listed below.

A. The Department will employ and retain in employment only those persons whose activities, associations, and backgrounds are consistent with the national interests, principles, and practices of the United States.

B. The use of the suspension and removal procedures authorized by 5 U.S.C. § 7532 shall be limited to cases in which the interests of the national security are involved. Maximum use of normal civil service suspension and removal procedures shall be used where, in the judgment of the General Counsel, such procedures are adequate and appropriate to support and promote proper security practices and to achieve the highest level of protection for NSI.

C. Individuals with access to NSI and/or sensitive information are subject to the provisions of all applicable laws, regulations, policies, and procedures of the Manual to protect and safeguard such information from unauthorized disclosure. Individuals shall not disclose NSI or sensitive information to any employee, to his or her counsel or representative, or to any other person not clearly authorized to have such information. Such a disclosure could compromise investigative sources or methods or the identity of confidential informants.

D. The Assistant Director for Counterespionage shall review adverse information relevant to an individual's access to NSI and may suspend, restrict, downgrade, propose denial, or propose revocation to an individual's access to NSI in accordance with the policies and procedures of the Security Manual.

E. Individuals will be appointed to a position in the Department only in accordance with the investigative requirements for suitability prescribed in the OPM Suitability Processing Handbook and the investigative requirements for access to classified NSI provided in this manual.

F. Citizens of foreign countries normally are denied employment with the Federal Government but can be employed under special provisions. Legal aliens, who meet requirements set by the OPM and who are proposed for affiliation with the Department, will undergo an appropriate background investigation.

G. Nominees for membership on Departmental advisory committees who require access to NSI must undergo an appropriate background investigation.

H. The Assistant Director for Counterespionage has the authority to grant eligibility for access to NSI for non-employees associated with the Department such as research associates, guest workers, and trainees.

I. Contractors requiring eligibility for access to NSI will be processed in accordance with the National Industrial Security Program Operating Manual and Chapter 37 of this Manual.

J. Work assignments to or visits by foreign nationals that involve access to restricted areas or to classified or other sensitive materials are discouraged. Access to NSI by a foreign national may be granted with sufficient justification, an appropriate background investigation, and review of the intended area of assignment or working area.

K. Individuals must inform the Counterespionage Division directly, or through the SSO, of adverse information pertaining to any officer or employee of the Department with access to NSI. In addition national security clearance holders are required to self report adverse information as above. After a thorough review of all pertinent information, the individual's eligibility for access to NSI may be suspended pending an investigation and review of the issues. After the appropriate investigation is completed, the individual's eligibility for access to NSI may be reinstated or revoked based on applicable laws, Executive Orders and federal regulations pertaining to national security.

Chapter 10. Position Designation

10.1. Position Risk and Sensitivity Designation

All positions in the Department of Commerce (Department) must be evaluated and assigned a sensitivity or a risk designation commensurate with the duties and responsibilities related to national security or to the efficiency of the service. The purpose of designating position sensitivity or risk level is to ensure that the incumbent undergoes the appropriate type of investigative processing and fulfills the requirements under Executive Order (E.O.) 10450, Security Requirements for Government Employment, and the Code of Federal Regulations (CFR) 5 Parts 731 and 732.

A. Responsibility for Position Designation.

1. The head of each operating unit or Department office, in consultation with his or her servicing human resources management office, shall ensure each employee's position in the operating unit or office is designated at the appropriate level of position sensitivity and/or risk, and this designation is clearly stated in the employee's position description. The criteria for risk designation are contained in Department Administrative Order (DAO) 202-731, Position Sensitivity for Personnel Suitability and Personnel Security Purposes. This order delegates to heads of operating units and servicing human resources managers the authority to designate the sensitivity and risk level for each position in their operating units or Department offices. Heads of operating units or Department offices may delegate this authority to subordinate managers and supervisors who have been delegated personnel management authority. See paragraph 10.2 below for a description of the designation of employee positions.

2. Positions established by contract in a Department facility or other direct association by a non-employee shall be designated with a position sensitivity and/or a risk level. Criteria for designating contract positions are discussed in paragraph 10.3 below. All contracts that involve access to classified information are processed through the Office of Security (OSY). For unclassified contract work, the responsibility for designating the risk level is shared by the contracting officer and operating unit management, and should be based on work performed in similar federal positions.

B. Basis for Position Designation.

1. 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 Department operations, also known as "the efficiency of the service."

   a. Sensitivity designations are given for national security positions and involve an assessment of one or both of the following considerations:

1) Duties and responsibilities of a position that directly or indirectly impact the interests of national security, including access to classified information under E.O. 12968 or similar authority, or access to sensitive, restricted facilities.
2) Information technology (IT) security functions that relate to the potential risks involving national security.

b. Risk level designations are given to all other positions and involve an assessment of one or both of the following considerations:
1) Duties and responsibilities of a position that directly or indirectly impact the Department's mission or the efficiency of the service, including consideration of public safety, the protection of public property, and public trust.
2) IT functions that relate to the potential risks involving the mission of the Department.

2. Upon completion of the assessment of both sensitivity and risk, the higher designation level of the two assessments becomes the minimum risk or sensitivity designation for the position and dictates the level of investigation required for the incumbent in the position.

C. Coding of Position Designation Levels.

Use of the Automated Position Designation Tool. In November 2008, OPM introduced a new Position Designation System and Automated Tool to simplify and automate the designation process. The Position Designation Tool is available on the OPM website at www.opm.gov/investigate. Its use is recommended for all agencies requesting OPM investigations and required for all positions in the competitive service, positions in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and career appointments in the Senior Executive Service. Agency personnel responsible for position designation are encouraged to visit the website.

D. Servicing Security Offices (SSO) shall maintain a record of the position designation levels for each position in the operating unit or office they support. The following position designation codes must be used when initiating an investigation into an individual's background. Paragraph 10.2 defines these designations.

Table 9 Coding of Position Designation Levels

LEVEL	CODING
Special-Sensitive (SS)	4N
Special-Sensitive IT	4C
Critical-Sensitive (CS)	3N
Critical-Sensitive IT	3C
Noncritical-Sensitive (NCS)	2N
Noncritical-Sensitive IT	2C

LEVEL	CODING
High Risk	6N
High Risk IT	6C
Moderate Risk	5N
Moderate Risk IT	5C
Low Risk	1N

IT – Information Technology Positions (2210 Series)

10.2. DESIGNATION OF EMPLOYEE POSITIONS

All employee positions in the Department require a risk or sensitivity designation. The level of investigation required for a position is determined by its risk or sensitivity designation. The level of investigation required by the sensitivity designation will normally take precedence over that required by the risk designation. Guidance for the designation of sensitive positions is outlined below.

A. National security (sensitive) positions may be designated Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive.

1. **Special-Sensitive (SS)** positions include any position that the head of an operating unit determines to be designated at a level higher than Critical-Sensitive (CS). This may be due to special requirements under an authority other than E.O. 10450 and E.O. 12968 such as Intelligence Community Directives that set investigative requirements and standards for access to Sensitive Compartmented Information (SCI) and other intelligence-related SS information.
2. **Critical Sensitive (CS)** positions have the potential for exceptionally grave damage to the national security. These positions may include access to Classified National Security Information (NSI), up to, and including, the Top Secret level.
3. **Noncritical-Sensitive (NCS)** positions have the potential for serious damage to the national security. These positions involve either access to Secret or Confidential NSI or duties that may adversely affect, directly or indirectly, the national security operations of the Department.

B. Non-national security (risk) positions may be designated High Risk, Moderate Risk, or Low Risk.

1. **High Risk** positions have the potential for exceptionally serious impact involving duties especially critical to the Department or a program mission with broad scope of policy or program authority. Examples include policy development and implementation, higher-level management assignments, independent spokespersons or non-management positions with authority for independent action, or significant fiduciary and procurement responsibilities.

2. **Moderate Risk** positions have the potential for moderate to serious impact involving duties of considerable importance to the Department or program mission with significant program responsibilities and delivery of customer services to the public. Examples include assistants to policy development and implementation, mid-level management assignments, non-management positions with authority for independent or semi-independent action, or delivery of service positions that demand public confidence or trust.
3. **Low Risk positions** involve duties that have a low or limited impact on the Department's mission or on the efficiency of the service.

C. Additional factors for determining the minimum position risk level.

1. **Uniqueness.** Factors unique to a particular position that are not accounted for elsewhere in the position designation process may cause adjustments to the position designation level. Examples include:
   a. Special investigative or law enforcement positions requiring possession and use of a firearm.
   b. Access to **or control of** Controlled Unclassified Information
   c. Access to sensitive financial records or control of an automated monetary system (i.e., key access entry).
   d. Few-of-a-kind positions with sensitive duties (i.e., special assistant to an agency head).
   e. Support positions with no responsibilities for preparation or implementation of sensitive program policies and plans, but which involve regular contact with and ongoing knowledge of all, or most of, such material (i.e., budget analyst).
2. **Uniformity.** Uniformity of position designations may be necessary because the authority level or program placement level may serve as a basis for the designation. For example:
   a. An agency head may adjust position designations at the same authority level to assure uniformity within the agency (i.e., managers of major agency programs at the same level of authority may be placed at the same level of risk).
   b. An agency head may place all positions within a program at the same position designation level if the risk to the program is such that, although no specific risks are associated with the position, the position involves work in an environment that can create a general risk to the program.
3. **Public Trust Positions.** Positions at the High Risk or Moderate Risk levels are designated as "Public Trust" positions. Such positions may involve policymaking, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust; and positions involving access to or operation or control of financial records, with a significant risk for causing damage or realizing personal gain. Therefore, these factors must be accessed to make a proper position designation determination.

10.3. DESIGNATION OF NON-EMPLOYEE POSITIONS (CONTRACTORS)

A. Position Designation for Non-Classified Contracts. The Contracting Officer's Representative (COR), in conjunction with operating unit management, SSO, and Security Contact, will review the work to be performed under contract and assign the highest risk designation to the entire contract in accordance with the criteria stated below. Accordingly, each contract employee will undergo investigative processing based on the contract's risk level designation (see paragraph 11.4 of this manual).

1. **High Risk.** A contract will be designated High Risk if it meets any of the following criteria:
   a. Work requiring continuous foreign travel of 90 days or more at any time during the performance of the contract under the auspices of the Department.
   b. Work involving functions or operations of the Department that are critical to the accomplishment of the mission of the Department.
   c. Work involving investigative, compliance, or senior-level auditing duties.
   d. Work involving fiduciary, public contact, or other duties involving the highest degree of public trust.
   e. Work involving automatic information networks and/or systems functions such as:
      1) Planning, directing, and implementing a computer security program.
      2) Planning, designing, directing, and operating a computer system that includes IT hardware, software, and/or data communications, regardless of the sensitivity or classification of the information stored on the system when there is no possible access to classified information.
      3) Access to a computer system, during the operation or maintenance process that could result in grave damage or in personal gain when there is no possible access to classified information.
   f. Any other work designated High Risk by the contracting officer and the head of the operating unit or Department office(s).
2. **Moderate Risk.** A contract will be designated Moderate Risk if it meets any of the following criteria:
   a. Work subject to little or no supervision by an appropriately cleared Federal Government employee that involves free access and movement during normal work hours within a Department facility that houses classified information or equipment.
   b. Work supervised by a Federal Government employee that occurs during restricted hours within a Department facility that houses classified or sensitive information or equipment.
   c. Work in which a contractor is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by Federal Government personnel whose position sensitivity is CS or above to ensure the integrity of the system.

d. Work requiring access to sensitive information (information protected under the Privacy Act or Title 13 of the U.S. Code).
e. Work involving foreign travel of less than 90 days' duration.

3. **Low Risk.** Work that does not fall into any of the categories noted above will be given a Low Risk designation.

B. Variance in Contract Responsibilities. In instances where there is a wide variance in the risk level of the work to be performed under one contract, individual contract employees can be processed at a Low Risk designation based on their duties when approved by the SSO. However, the contract document must specifically apply controls to ensure that the work of persons in the Low Risk positions will not overlap with that for the Moderate and/or High Risk positions. The contract will identify the number of employees to be processed at the Low Risk designation and will specify the duties of these positions. An example of such a case is custodial work where some contract employees perform work that is not supervised during security hours (weekdays 6:30 AM to 5:30 PM) in a facility that houses classified information, while others may work under close government supervision during normal work hours. The entire contract might be designated High Risk or Moderate Risk because of the first group of contract employees, but those contract employees whose work would be Low Risk would be processed with the appropriate background investigation. The contract must meet control obligations to ensure that there is no overlap of work duties between the two groups.

C. Position Designations for Classified Contracts. Classified contracts are handled under the auspices of the Department of Defense National Industrial Security Program (NISP). Generally, contract employees requiring access to NSI are not processed through the Department's Personnel Security Program, but through the NISP process. For guidance on classified contracts, refer to Chapter 37, Industrial Security, of this manual.

D. Position Designations for Other Non-employee Positions.

1. Experts and consultants are subject to the same security requirements as regular employees of the Department. Because experts and consultants are paid at a level equivalent to a GS-13 or above, such positions should be evaluated based on Public Trust criteria. If a position is not sensitive, an expert or consultant should be evaluated as an employee for a High Risk or Moderate Risk position would be.

2. Guest workers, research associates, trainees, long-term visitors, and other similar types of non-employees associated with the Department usually serve in a Low Risk capacity. There are no specific criteria for evaluating their involvement under risk designation criteria; however, the determination should take into account the potential impact or damage that the non-employee's interaction could cause. If the involvement of these non-employees falls within the generic description of a sensitive position, the manager of the operating unit involved must advise OSY in accordance with this chapter of the Security Manual.

10.4. POSITION DESIGNATION CODE—CHART SUMMARY

The following chart provides the position designation codes for risk and sensitivity along with the impact on the integrity of the federal service and the national security. If the national security designation is rescinded, the position reverts to the risk designation coding.

Table 10 Position Designation Code—Chart Summary

POSITION DESIGNATION	IMPACT ON FEDERAL SERVICE OR NATIONAL SECURITY
4: SS or **4C:** SS IT	Potential for inestimable damage to the national security. Used for positions that the head of an operating unit designates at a level higher than CS because of special requirements for access to SCI or other intelligence-related SS information.
3: CS or **3C:** CS IT	Potential for exceptionally grave damage to the national security. These positions may include access up to, and including, Top Secret information; investigative duties, the issuance of personnel security clearances, or duty on personnel security boards; or other positions related to national security, regardless of duties, that require the same degree of trust.
2: NCS or **2C:** NCS IT	Potential for serious damage to the national security. These positions involve either access to Secret or Confidential NSI or materials or to duties that may adversely affect, directly or indirectly, the national security operations of the Department.
6: High Risk or **6C:** High Risk IT	Potential for exceptionally serious impact involving duties especially critical to the Department or a program mission with broad scope of policy or program authority.
5: Moderate Risk or **5C:** Moderate Risk IT	Potential for moderate to serious impact involving duties of considerable importance to the Department or program mission with significant program responsibilities and delivery of customer services to the public.
1: Low Risk or **1C:** Low Risk IT	Positions involve duties that have a low or limited impact on the Department's mission or on the efficiency of the service.

Chapter 11. Investigative Processing

11.1. Security and Suitability Investigations

Every position in the Department of Commerce (Department) requires some level of investigative processing for suitability and/or security. This chapter covers processing procedures required for security and suitability investigations and the relationship to position sensitivity and risk designations.

All background investigations will be processed through the Office of Personnel Management (OPM) website using Electronic Questionnaires for Investigations Processing (e-QIP). No security office or human resources office will process hard copies of SF-85, SF-85P, or SF-86.

A. Introduction.

1. Consistent with Executive Order (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, the following standards are established for national security and suitability investigations of all individuals working for or on behalf of the Executive Branch of the Federal Government or who seek to perform work for or on behalf of the Executive Branch, and individuals with access to federally controlled facilities and information systems.
2. When designated for use to conduct investigations, the new standards herein supersede the standards previously approved by the President under E.O. 12968, "Access to Classified National Security Information," dated August 2, 1995. To the extent there is any conflict between the new standards and those previously approved, the new standards will prevail.
3. The Department or any of its bureau's may not establish additional investigative requirements that exceed these standards without the approval of the Director of National Intelligence who is the Security Executive Agent or the Director of OPM who is the Suitability Executive Agent, as appropriate. The Executive Agents shall ensure that any approval to establish additional requirements shall be limited to circumstances where additional requirements are necessary to address significant needs unique to the agency involved or to protect national security, and ensure that security and suitability investigations remain aligned.

B. Investigative Requirements.

1. Suitability investigations provide an assessment of an individual's likelihood to promote the efficiency and integrity of the Department's operations when filling a particular position. Security investigations are used to determine whether employment or retention in employment is consistent with national security interests. The investigative process for both types of investigations gathers information and evaluates the background of employees and non-employees associated with the Department. The findings or facts ascertained through security investigations are used

to determine eligibility for access to Classified National Security Information (NSI) (covered in Chapter 12) or for special access program determinations (covered in Chapter 15). General guidance showing the minimum type of security and suitability investigation for each sensitivity or risk level is provided in this chapter, for employees and non-employees.

2. Employees appointed to any Departmental position will be subject to suitability investigation. Employees are subjected to suitability investigations upon initial appointment to the federal service and upon reappointment after a break in service of 24 months or more. Current federal employees appointed to Departmental positions may be subjected to further investigation if the position to which they are being appointed carries a higher risk/sensitive designation than that for which they were previously investigated. Employees will be subject to investigation for access to NSI prior to, or immediately following, Entrance on Duty (EOD) in accordance with the provisions of this Security Manual. In general, the type of investigation conducted is based on the position's sensitivity or risk level designation.
3. Many non-employees are subject to investigation if they have an official association with an operating unit or Departmental office. In general, the type of investigation conducted, if required, is based on the risk associated with the individual's work and the anticipated period of association with the Department.

C. Protection of Investigative Sources and Materials. Applicable regulations that pertain to safeguarding NSI and to handling investigative reports will be strictly observed. No protected information, nor any information that might compromise investigative sources or methods or otherwise identify confidential sources, shall be disclosed to any employee, to his or her counsel or representative, or to any other person not clearly authorized to have the information.

D. Release of Investigative Reports. Personal information collected from employees, applicants, and non-employees is protected by the **Privacy Act of 1974** (Privacy Act). Reports of investigation may be released only in accordance with the provisions of the **Privacy Act** or **Freedom of Information Act (FOIA)**. To obtain a copy of the investigative report, the subject of the investigation must submit a **Privacy Act** request directly to the agency conducting the investigation. For example, for the Department, OPM is the investigative agency that conducts most of the background investigations for sensitive and risk-designated positions. The subject of the investigation would have to submit a **FOIA** request directly to OPM to obtain a copy of the investigative report.

E. Reinstatement of Terminated Employees. No person whose employment has been terminated by the Department under the provisions of **5 U.S.C. § 7532**, **E.O. 10450, as amended**, **E.O. 12968**, **E.O. 13467**, or any other security or loyalty program, shall be reinstated, restored to duty, or reemployed in the Department unless the Secretary finds that such employment is clearly consistent with the interests of the national security. No person whose employment has been terminated by any department or agency, other than the Department, under **5 U.S.C. § 7532**, **E.O.10450, as amended**, **E.O. 12968**, **E.O.**

13467, or any other security or loyalty program, shall be employed in the Department unless the Secretary finds that such employment is clearly consistent with the interests of the national security and unless the OPM determines that the person is eligible for such employment. The finding of the Secretary and the determination of OPM shall be made a permanent part of the personnel record of the person concerned.

F. **Breaks in Service/Employment Less Than 24 Months.** Subjects who have a continuous (not cumulative) break in service/employment of 24-months or less will be subject to the minimum of a fingerprint check, when returning to work for or on behalf of the Government. Their current investigation on record will be used unless a new investigation is required by the Continuous Evaluation/Reinvestigation standard results of fingerprint checks are adverse; a review of indices of prior investigations; and adjudications indicate the subject may no longer satisfy the applicable suitability or security adjudication standards; or a higher-level investigation is required for the new position.

G. **Breaks in Service/Employment Over 24 Months.** Subjects who have a continuous (not cumulative) break in service/employment greater than 24-months must complete an updated e-QIP and undergo the investigation required by their position designation when returning to work for or on behalf of the government.

11.2. TYPES OF SECURITY AND SUITABILITY INVESTIGATIONS

The following types of investigations are currently used for making security and suitability determinations in the Department. These investigations are prescribed by OPM. When preparing request packages for investigations, supervisors should refer to Section 11.5, Submitting Investigation Requests, of this chapter.

A. **National Agency Check (NAC).** The NAC consists of record searches of national, state, and local law enforcement and investigative indices. The NAC may also involve a credit check conducted by the Office of Security (OSY). OSY conducts NACs as part of the pre-appointment process when a request for temporary eligibility for access is received. (Although a pre-appointment check consists of a search of national indices by OSY, the terms "NAC" and "Pre-Appointment Check" are not interchangeable because not all NACs are conducted prior to appointment.)

Note: The NAC is not an investigative product that can be requested, however, it is a part of most investigations.

B. **Special Agreement Check (SAC).** The SAC consists of a modified NAC and includes OPM, Department of Defense, and Federal Bureau of Investigation (FBI) checks. OPM conducts SACs for the Department. SACs are used to obtain background information on non-employees such as short-term trainees, students, or other individuals requiring temporary access to Departmental facilities.

C. **National Agency Check and Inquiries (NACI).** The NACI consists of a NAC plus written inquiries and record searches covering employment, residence, education, during the past five years.

D. **Access National Agency Check and Inquiries (ANACI).** The ANACI consists of the NACI plus a check of all local law enforcement agencies where the subject has lived, worked, or gone to school in the past five years, and a credit search over the preceding seven years. The ANACI is the minimum requirement for granting eligibility for access to NSI at the Secret level for non-critical sensitive positions.

Note: These investigations will provide issue-triggered enhanced subject interviews, with added issue resolution.

E. **National Agency Check with Law and Credits (NACLC).** The NACLC is used as the initial investigation for contractors at the Confidential, Secret, and Department of Energy "L" access levels. It is also used as the reinvestigation product for both contractors and federal employees at the Secret access level for non-critical sensitive positions. The NACLC consists of the basic NAC plus a records search covering all residence, employment, education, and credit history during the most recent five-year period; all locations of admitted arrest going back to the individual's 18th birthday; and a credit check over the past seven years.

Note: These investigations will provide issue-triggered enhanced subject interviews, with added issue resolution.

F. **Childcare National Agency Check with Inquiries (Childcare NACI).** For purposes of childcare personnel the NACI will be requested on the SF-85 (Code 2 and 8 on the extra coverage of the Agency Use Book in e-QIP). The investigation consists of state criminal history repository (SCHR) checks for all states of residence. Other coverage elements, such as a credit search, are available by request, or when certain background conditions exist. The NACI with extra coverage meets the intent of 42 U.S.C. §13041 as well as the minimum suitability investigation requirements directed for federal employment under E.O. 10450, as amended.

G. **Minimum Background Investigation (MBI).** The MBI consists of a subject interview, credit history, and all the components of a NACI covering the most recent five-year period for law enforcement checks and seven years for credit checks. The MBI is the investigative produce for a Moderate Risk position.

Note: An MBI may also be used as a national security investigation, when conducted on an SF-86, if a Secret clearance is required and a subject interview will benefit the investigative process for the Secret clearance.

H. **Background Investigation (BI).** The BI consists of a NACI, subject interview, record searches, credit check, and personal interviews with selected sources covering employment, residence, education, and law enforcement agencies during the most recent five-year period but not less 24 months with a credit check up to seven years. The BI is the minimum investigation for a High Risk position.

I. **Single Scope Background Investigation (SSBI).** The SSBI consists of a NACI; subject interview; written inquiries; record searches; credit check; personal interview with selected sources covering employment, residence, education, and law enforcement

agencies during the most recent ten-year period; plus a NAC on the subject's spouse or other individuals bound to the subject by economics, affection, or living arrangements. A credit check will be made on the past seven years. The SSBI is the minimum investigation for Top Secret clearances for Critical Sensitive positions or Special Sensitive positions when eligibility for access to Sensitive Compartmented Information (SCI) is required.

J. **Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR).** The SSBI-PR is the 5-year periodic reinvestigation for Critical and Special Sensitive positions no matter the level of clearance granted. The SSBI-PR consists of no less than an updated SF-86 and review of related personnel security files. In addition, a NAC, subject interview, record searches, credit check, and resolution of any issues arisen since the last investigation or during the preceding five years, whichever is longer, is ordinarily warranted.

K. **Periodic Reinvestigation (PRI).** The PRI is a 5-year reinvestigation for Public Trust Positions at the High Risk Level. The PRI consists of an updated SF-85P, NAC for the subject, credit check, subject interview, law enforcement checks on all locations of 4 months or more, and contacted inquiries. The investigation covers a 5-year period of time.

11.3 INVESTIGATIVE REQUIREMENTS FOR APPLICANTS AND EMPLOYEES

A. **General Requirements.** The minimum type of investigation to be performed depends on the designation of the position to which an individual is appointed. The Servicing Human Resources Management (SHRM) or local administrative office, as appropriate, will provide the necessary investigation-related forms and instructions to applicants and/or new employees in accordance with the level of investigation required for the risk/sensitivity designation of the position.

Note: Position designation and applicable investigative requirements are outlined in Chapter 10, Position Designation, of this manual.

B. **National Security (Sensitive) Positions.** The Special-Sensitive, Critical-Sensitive, and Non-Critical Sensitive designations are the national security designations for sensitive positions in the Department. Each of these designations requires a favorable pre-appointment check conducted by OSY before appointment. The pre-appointment check is conducted to verify and adjudicate a previously completed investigation, to establish a temporary investigative basis for appointment, or to provide a basis for waiving the investigative requirement for a Critical-Sensitive position before appointment. A pre-appointment check will normally require a minimum of three to five working days to complete. Additional time may be required depending on the facts in the particular case or on other elements beyond the control of the Department. Operating officials should plan accordingly and initiate pre-appointment checks at the earliest possible date after selection and prior to the desired EOD date. When preparing the request package for any of the following positions, supervisors of

employees being investigated should refer to section 11.5, Submitting Investigation Requests.

C. **Special-Sensitive Positions.** No person shall be appointed, detailed, or assigned to a national security position designated Special-Sensitive until a satisfactory pre-appointment check has been completed and a SSBI has been scheduled with OPM. OSY will advise the SHRM when the SSBI requirement has been met and the pre-appointment has been approved.

1. The pre-appointment investigative requirement may not be waived for appointment to positions designated Special-Sensitive (see 5 CFR Part 732.202).
2. In addition to a successfully adjudicated investigation, any person under consideration for a position designated Special-Sensitive due to special access program considerations also must meet the special access clearance requirements set forth in Chapter 15, Special Access.
3. The incumbent of each Special-Sensitive position shall be required to submit the appropriate forms to OSY to initiate an SSBI five years after completion of the previous investigation, or at least once during each succeeding five-year period, or when requested by OSY. OSY will notify an employee's supervisor of this requirement through his or her Servicing Security Office (SSO) prior to the employee's five-year anniversary.
4. An employee occupying a Critical-Sensitive position at the time that it is upgraded to a Special-Sensitive designation as the result of an unanticipated change in duties, may continue to occupy the position upon the satisfactory completion of an SSBI and credit check. However, access to NSI in the Special-Sensitive program will not be permitted until the appropriate investigation has been completed and favorably adjudicated. The appropriate investigation must be initiated as an expedited case (see Paragraph 11.5, Processing Investigations) within 14 days of the Special-Sensitive designation.
5. An employee occupying a non-sensitive (Risk) position when the position is upgraded to a Special-Sensitive designation, as the result of an unanticipated change in duties, may not occupy the Special Sensitive position prior to the favorable completion of the SSBI. Normally, the employee or individual will be detailed to another position or to unclassified duties pending completion of the investigation.
6. An employee, a transferee, or an applicant with an SSBI less than five years old may not occupy a Special-Sensitive position until OSY has verified and favorably adjudicated the investigation. The individual may need to certify in writing that there has been no change in the relevant information since the individual's last background investigation. OSY, in consultation with the SHRM management office and the management supervisor, will coordinate the appointment and EOD on a case-by-case basis.

D. Critical-Sensitive Positions.

1. No person shall be appointed, detailed, or assigned to a position designated Critical-Sensitive until a satisfactory pre-appointment check has been completed and a SSBI has been scheduled with OPM. Commitment to such an appointment may not be made until OSY advises the SHRM that the SSBI requirement has been approved.

2. The Director for Security, or designee, however, may waive the requirement for the prior completion of a SSBI for a Critical-Sensitive position that requires access to Secret or Top Secret information in an emergency situation when deemed in the national interest. The waiver can be approved only after a SSBI has been scheduled with OPM and credit check has been favorably completed. Also, a National Crime Information Center/National Law Enforcement Telecommunication System check must be completed favorably. If the required investigation is not favorably adjudicated, access to Secret or Top Secret information will be immediately terminated, along with any assignment requiring an access eligibility approval. In consultation with OSY, the SHRM office and the operating unit will ensure the individual is appointed to another position or terminated from employment.

3. In addition to a successfully adjudicated investigation, any person under consideration for a position designated Critical-Sensitive, because of the need to access Secret or Top Secret information, also must meet other security clearance requirements set forth in Chapter 12, Access to NSI.

4. The incumbent of a Critical-Sensitive position shall be required to submit the appropriate forms to the SSO via e-QIP to initiate a SSBI, when Secret or Top Secret access is required, five years after completion of the previous investigation or at least once during each succeeding five years, or when requested by OSY. OSY will notify the employee's supervisor through the SSO when there is a need to initiate a five-year reinvestigation.

5. An employee occupying a Non-Critical Sensitive or any Risk designated position at the time that it is upgraded to a Critical-Sensitive designation requiring a national security clearance (at the Secret or Top Secret level), as the result of an unanticipated change in duties, may continue to occupy the position upon the satisfactory completion of a SSBI and credit check; however, the SSBI must be initiated as an expedited case within 14 calendar days of the Critical-Sensitive designation. If the required investigation is not favorably adjudicated, the SHRM office and the operating unit, in consultation with OSY, will ensure the individual is appointed to another position that does not require access to NSI.

6. An employee, a transferee, or an applicant with an SSBI less than five years old may not occupy a Special-Sensitive position until OSY has confirmed a favorable adjudication of the investigation. The individual may need to certify in writing that there has been no change in the relevant information since the individual's last

background investigation. OSY, in consultation with the SHRM office and the management supervisor, will coordinate the appointment and EOD on a case-by-case basis.

7. Appointment to a Critical-Sensitive position may be made based on a SSBI that is more than five years old when a favorable pre-appointment check is obtained; however, a SSBI must be initiated within 14 calendar days of the employee's appointment to the position if the employee has had a break in service of more than 24-months or if the SSBI is more than five years old, provided that the employee certifies in writing that there has been no change in the relevant information provided since the employee's last background investigation, an appropriate records check reveals no unfavorable information, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by E.O. 12968.

E. Non-Critical Sensitive Positions.

1. Positions requiring access at the Secret level (without risk factors that elevate the position to Critical-Sensitive) are identified as Non-Critical Sensitive. No person shall be appointed, detailed, or assigned to a position designated Non-Critical Sensitive until a pre-appointment check, including a credit check, has been satisfactory completed. Retention in the Non-Critical Sensitive position is contingent on the subsequent completion of an ANACI that has been favorably adjudicated. The ANACI must be initiated no later than 14 calendar days after an employee's appointment to the position and EOD. If the required investigation is not favorably adjudicated, appointment to the position must be immediately terminated. OSY, in consultation with the SHRM office and the operating unit manager, will then coordinate the appointment of the individual to another position or terminate the employment.

2. In addition to a successfully adjudicated investigation, any person under consideration for a position designated Non-Critical Sensitive, because of the need to access Secret information, also must meet other security clearance requirements set forth in Chapter 12, Access to NSI.

3. An employee occupying a non-sensitive (Risk) position at the time that the position is upgraded to a Non-Critical Sensitive designation, as the result of an unanticipated change in duties, may continue to occupy the position subject to the satisfactory completion of a pre-appointment check by OSY. If employees do not have a previously completed, favorable NACI, they may not continue to occupy the position until a NACI has been completed and favorably adjudicated. The investigation must be initiated within 14 calendar days of the position's upgrade to a Non-Critical Sensitive designation. During the conduct of pre-appointment checks, if an NACI or higher investigation, requested on an SF-86, Questionnaire for National Security Positions, is located and has been favorably adjudicated, no further processing beyond the pre-appointment is required. If the required

investigation is not favorably adjudicated, the SHRM office and the operating unit, in consultation with OSY, will ensure the individual is appointed to another position that does not require access to NSI.

4. An employee, a transferee, or an applicant who has a previously completed investigation, may not be offered or appointed to a Non-Critical Sensitive position until OSY has verified the level and favorable adjudication of the prior investigation, unless an upgraded investigation has been initiated. The appointment can be made if the individual has remained employed by the same employer during the period in question, the employee certifies in writing that there has been no change in the relevant information provided since the employee's last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by E.O. 12968.

F. Reinvestigations/Continuous Evaluation.)

1. All positions designated "Sensitive" (Special Sensitive; Critical Sensitive; Non-Critical Sensitive), require reinvestigation/continuous evaluation, in accordance with E.O. 12968, and E.O. 13467.

2. All positions designated "Public Trust," which includes Moderate and high Risk positions require five year recurring reinvestigation in accordance with E.O. 13467 and 5 CFR 731 (as amended).

G. Risk Positions (Non-Sensitive). All DOC positions, regardless of their sensitivity designation, must have a determination of risk. Instructions on the designation of risk levels and the factors used to determine risk level can be found in Chapter 10, Position Designation, of this manual.

1. Appointments to risk positions are not normally contingent on the completion of an investigation prior to appointment; however, continued employment in these positions is subject to the satisfactory completion of an appropriate investigation. In addition, Low Risk and most Moderate Risk positions do not require a pre-appointment check prior to appointment; however, High Risk positions and Moderate Risk positions in the information technology (IT) occupations and those with "global access" to an automated information system require favorable pre-appointment checks prior to appointment.

   a. The SF-85, Questionnaire for Non-Sensitive Positions, is used to request investigations for Low Risk positions. The SF-85P, Questionnaire for Public Trust Positions, will be used to request investigations for Moderate and High Risk positions. The SF-85 and SF-85P must be completed using the OPM e-QIP system.

   b. Appointments for a period of more than 180 days to intermittent, temporary, or seasonal positions, or of non-U.S. citizens being employed outside the United States shall be processed as determined by the risk level of the position and the

previous investigation of the selectee, except as otherwise determined by the SHRM.

2. Individuals employed in High Risk positions, or Moderate Risk positions in the IT occupations, and those at the Moderate Risk level with "global access" to an automated information system, shall be subject to reinvestigation as deemed necessary, but not less frequently than once every five years.

3. Applicants for positions designated at the Low or Moderate Risk level will not normally require a new background reinvestigation provided the applicant has previously undergone the required level of investigation with favorable results and has not had a break in federal service. Positions at the Moderate and High Risk shall be subject to a favorable pre-appointment check prior to appointment, regardless of a previously completed investigation.

   a. The SHRM office will review the applicant's Official Personnel Folder (OPF), and/or contact the previous federal employer or OPM to verify previous completion of the required level of investigation. If the SHRM is unable to verify investigative processing by these means, the OSY may be contacted to assist in obtaining the information.

   b. Based on the name, social security number (SSN), and date and place of birth of the subject in question, verification will be made by the OSY through a computer link between the OSY and OPM's investigative database.

4. When an employee transfers from another federal agency to a non-sensitive position in the Department and the appropriate investigation initiated by the relinquishing agency has not been completed, the SHRM must submit a request to OPM to obtain the results of any previously completed or pending investigation. The request should include the individual's original application form (OF-612), or resume, from which the employee was appointed to the Department, any information received by voucher or other means that would tend to identify the ongoing investigation, and a transmittal letter stating that an investigation had been initiated previously in connection with the appointment in the relinquishing agency. The letter must identify the relinquishing agency, indicate the type of appointment and authority for appointment in the Department, and request that the results of the investigation be forwarded to the requesting SHRM office.

H. Investigative Requirements for Employment of Non-U.S. Citizens

1. **Non-U.S. Citizen Appointment to Non-Sensitive Positions for 90 days or less.**

   a. A non-U.S. citizen may be employed in a non-sensitive (Risk) position for a period of 90 days or less only after the completion of the requirements set forth in section 11.5, Submitting Investigation Requests. For purposes of this subparagraph, technical or scientific positions that do not require access to NSI or to restricted areas and that do not involve administrative or policy-forming responsibilities may be considered Low Risk positions.

b. Pre-appointment processing for non-U.S. citizens in non-sensitive positions will be initiated as prescribed in section 11.5, Submitting Investigation Requests, at least 30 days prior to the proposed appointment. The pre-appointment request must identify the individual as a non-U.S. citizen, request concurrence in the proposed appointment, and transmit an SF-85, Questionnaire for Non-Sensitive Positions, containing the non-U.S. citizen's biographical information. A fingerprint card (FD-258) also is required if the non-U.S. citizen is residing in the United States at the time of application or has had previous residences in the United States that cumulatively amount to a year or more. The appointment may not be made until concurrence is received from the Director or delegated designee. It will not be necessary in such cases to initiate the post-appointment investigation required for non-sensitive positions.

2. **Non-U.S. Citizen Appointment to Non-Sensitive Positions for more than 90 Days.**
   a. **Employment up to one year:** A non-U.S. citizen may be appointed to a non-sensitive position in the Department for a period of more than 90 days not to exceed one year only after a favorable BI has been completed. When recommended by the head of the operating unit concerned and approved by the Chief Financial Officer and Assistant Secretary for Administration (CFO/ASA), a scientific or technical position that does not involve administrative or policy-forming responsibilities and that does not involve access to NSI or to restricted areas may be considered a Low Risk Position.
   b. **Employment for more than one year:** A non-U.S. citizen may be re-appointed after a one-year appointment or may be appointed initially to non-sensitive positions for indefinite periods (exceeding one year) after the completion and adjudication of a favorable BI, provided that the non-U.S. citizen has formally declared his or her intention in writing to become a U.S. citizen prior to the making of such an indefinite appointment. When recommended by the head of the operating unit concerned as being in the best interests of the Government and approved by the CFO/ASA, a U.S. citizen or a non-US citizen who has not declared an intention of becoming a U.S. citizen and who has been given a one-year appointment under conditions described above may be re-appointed for a temporary appointment of one year or less.

3. **Non-U.S. Citizen Appointment to a Sensitive Position.** A non-U.S. citizen appointed to a non-sensitive position, as prescribed above, will be eligible for assignment to a sensitive position only after having been employed in the Department for a continuous period of not less than three years, demonstrating to the satisfaction of the Director, or designee, a continuing and sincere desire to become a U.S. citizen. If appointment to a sensitive position requires access to NSI, the clearance will be temporary. There must be compelling reasons in furtherance of the Department's mission, where the subject possesses a special expertise, and access is limited for specific programs, projects, contracts, licenses,

certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of NSI than the United States Government has determined may be releasable to the country which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of the subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued. A final security clearance shall only be granted to individuals who are U.S. citizens, and for whom an appropriate investigation has been completed, and whose personal and professional history affirmatively indicates loyalty to the U.S., strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of NSI.

11.3. Investigative Requirements for Non-Federal Employees.

The following information describes the investigative requirements for non-federal employees. Guidelines for initiating the investigations are provided in Section 11.5, Submitting Investigation Requests. For non-federal employees in a Low Risk position for 30-180 days a SAC will be the minimum investigation accepted. For 30 days or less a fingerprint check will be conducted. All other non-federal employee investigations will be determined by the position designation. Non-Federal Employees include non-paid volunteers who work for or on the behalf of the Department.

A. **Contractors.** Investigative requirements for contract personnel are divided into two major categories: unclassified contracts and NSI contracts. Unclassified contracts involve no access to NSI. Classified contracts involve access to NSI and are referred as Classified, or Sensitive contracts.

1. **Classified Contracts.** All non-employees who require a security clearance to meet contract or other obligations with the Department will be investigated and granted a security clearance in accordance with the provisions of the National Industrial Security Program Operating Manual (NISPOM) and this chapter. Security clearances are required for all contract work involving access to NSI. Security clearances for personnel performing work on a classified contract must be granted their clearance by the Defense Industrial Security Clearance Office in accordance with the NISPOM. On a case-by-case basis, however, experts or consultants performing work on a project or program requiring access to NSI may be granted a security clearance by the Director, or delegated designee, for short-term classified work. See Chapter 37 of this manual for further guidance.

2. **Unclassified Contracts.** All other contract personnel must undergo investigative processing according to the risk level of the contract. The Contracting Officer's Representative (COR), in conjunction with operating unit management and Security Contact, is responsible for assigning a risk designation to each contract where work will be performed in the Department. Within each contract, the

contracting officer must include information that defines the investigative requirements associated with the contract's risk level. Sample Language is included in Section 3 of the Commerce Acquisition Manual. The COR is responsible for initiating the investigation request package for a contract employee. The request package is submitted to the SSO through the Security Contact. The following procedures describe the investigative requirement for contract personnel by risk level.

a. A contract at the High Risk level requires a pre-employment check prior to EOD, with a BI initiated no later than three working days after the start of the person's performance on the contract.
b. A contract at the Moderate Risk level requires a pre-appointment check prior to EOD and the initiation of an MBI no later than three working days after the start of the person's performance on the contract.
c. At the Low Risk level, requirements are based on the expected duration of the contract and on the nature of the work to be performed and a pre-appointment check prior to EOD. All Low Risk positions in IT will be subject to a NACI regardless of the contract's duration. All other Low Risk positions over 180 days in duration will be subject to a NACI. Low Risk contracts with a duration of less than 180 days require at the minimum a SAC. At the discretion of the Security Contact, a NACI may be requested for Low Risk contracts of short duration where unusual circumstances exist and warrant the processing for the contractors involved.

B. Guest Workers, Research Associates, Experts, Consultants, Long-Term Visitors, and Trainees.

1. This paragraph prescribes the security requirements, known as "security assurance," for guest workers, research associates, experts, consultants, long-term visitors, trainees, and other individuals who have similar associations with the Department. The provisions of DAO 202-311, Voluntary and Uncompensated Services; DAO 202-304, Employment of Individual Experts and Consultants; and DAO 207-12, Foreign National Visitor and Guest Access Program, are also pertinent to this subject and shall be applied by all operating units.

2. Functions performed by these non-employees are assigned risk designations at the Low, Moderate, or High level. U.S. citizens serving in positions who expect to remain with the Department for more than 180 days shall be subject to investigative processing.

3. Completion of the security assurance processing requirements set forth in this chapter does not automatically permit visitors or other categories of non-employees associated with the Department to have access to NSI or to restricted areas. Security clearances for such purposes, as distinguished from security assurances, must be obtained in accordance with applicable security regulations.

4. Although the Department allows guest workers, research associates, experts and consultants, and trainees access to its facilities, the final authority for determining the acceptability of such individuals belongs to the Department. The operating unit head shall make certain that the provisions of this Security Manual are met before assigning or agreeing to assign an individual to a Departmental facility within his or her unit, and may prescribe additional control measures as necessary.
5. If the duties of a guest worker, research associate, or trainee appear to fall within the generic description of a National Security position (see Chapter 10 of this manual), the head of an operating unit must provide a written statement to that effect to OSY through the delegated SSO. The statement should include information describing the particular type of involvement that appears to create a situation similar to that for a sensitive position.

C. U.S. Citizens.

1. **180 to 365 Days.** A NACI is required for U.S. citizens associated with the Department for more than 180 days but less than 365 days. The NACI must be requested prior to the 180th day of the individual's association with the Department.
2. **30 to 180 Days.** A SAC may be requested for U.S. citizens associated with the Department from 30 to 180 days when there is a potential for increased risk.

D. Non-U.S. Citizens.

1. **More than One Year.** A NACI is required for non-U.S. citizens associated with the Department for more than one year. The NACI must be initiated within three working days of the individual's beginning association with the Department.
2. **Less than a Year.** A SAC is required for non-U.S. citizens who expect to remain with the Department for more than 10 working days within 12 consecutive months. The SAC must be initiated within three days of the individual's beginning association with the Department.

E. Non-Federal Short-Term Visitors on Official Business. Short-term visitors are defined as non-federal employees on official business to Departmental facilities, making visits that do not extend beyond 30 working days for citizens or 10 working days for non-citizens within a consecutive 12-month period, and that do not involve access to NSI or to restricted areas. No security assurance processing is required for short-term visitors, but managers of operating units to be visited shall make definitive arrangements, such as designating escorts, to prevent accidental access to restricted areas or to NSI during these visits. In general, however, assignments or visits of foreign nationals that entail potential access to restricted areas or to NSI should be discouraged.

F. Projects Sponsored by Other Federal Agencies. When a project being conducted in a Departmental facility is being carried out by another federal agency, the investigative

processing requirements of the sponsoring agency shall apply unless other arrangements are made.

G. **Processing Membership for Departmental Advisory Committees.** Security and suitability processing is required for all nominees for membership on Departmental advisory committees who require access to NSI. Committee Liaison Officers for each operating unit coordinate the process of obtaining access to NSI. The procedures are set forth in the Committee Handbook and this chapter.

H. **Childcare Workers Employed at Commerce Facilities.** In compliance with 42 U.S.C. § 13041, employees of childcare centers located in Department facilities must be subjects of background checks. The General Services Administration (GSA) conducts such checks (CNACI) on childcare providers when the childcare center is located in a GSA-controlled facility. Currently, there are Departmental facilities using GSA-approved childcare contractors as well as childcare contractors not processed by GSA. The Security Contact or SSO must verify that appropriate background checks were conducted on each employee of the contract provider. When a GSA-approved contractor is not used, the Security Contact or SSO is responsible to ensure that appropriate checks have been conducted. As outlined in 42 U.S.C. § 13041, the minimum criminal history checks for applicants will be a fingerprint check of the records in the Identification Division of the FBI and a check of the state criminal history repositories of all addresses listed on the application for employment as either current or former residences. In addition, the application for employment will contain a question asking whether the individual has ever been arrested for or charged with a crime involving a child, and, if so, the manager will require a description of the nature of the arrest or charge. The application shall state that it is being signed under penalty of perjury. Where this language is not included on the application for employment, a separate sheet with this information should be attached.

The SSO will work with the COR to ensure that the CNACI is initiated for persons being hired with childcare responsibilities at Departmental facilities. This investigation must be used to comply with the Public Law. An operating unit may hire a staff person provisionally prior to the completion of the required background check provided that, when caring for children, the uncleared individual must at all times be within the sight and under the supervision of a staff person whose background check has been successfully completed and the Childcare NACI has been initiated prior to, or on, the appointment date.

11.4. SUBMITTING INVESTIGATION REQUESTS.

A. **Introduction.** SSOs have the responsibility to confirm that all security-processing requirements within his or her jurisdiction are met. The initial responsibility for preparing security and suitability request packages for employees or applicants is usually that of the SHRM officer. The SSO shall assist the SHRM office with regard to the processing of paperwork for security and suitability positions. The Contracting Officer or COR has the initial responsibility for contract workers and their request packages. Managers or other

officials who represent the Department in interactions with non-employees have the initial responsibility for preparing their request packages. The SSO is responsible for tracking all investigations for NSI positions within delegated respective jurisdiction. In connection with these responsibilities, the following guidelines and procedures are provided to ensure a uniform personnel security investigative program among the operating units and the Department.

B. Investigations.

1. **Pre-Appointment Check (Sensitive, High Risk, and certain IT-related Moderate Risk positions).**

   a. **Requirement**. A pre-appointment check is optional for most positions; however, it is required for Moderate Risk positions in the IT occupations, positions that afford "global access" to information systems, and all Sensitive and High Risk positions. These checks will include favorable NAC or NCIC checks for criminal history, FBI fingerprint check, and credit check.

   b. **Procedure.** The SHRM office initiates the individual into the OPM website to complete his or her security forms online via e-QIP, in advance of the EOD date. The individual completes all forms, obtains a fingerprint card (if outside the local Washington, DC, area) from the SSO (fingerprints if outside the local DC area may be taken at their local police station), and returns the signature pages from e-QIP and completed fingerprint card to the SHRM office. The SHRM office sends the completed package to OSY headquarters for processing within three calendar days of the date the applicant certifies his or her e-QIP forms.

   c. **Request Package**. The pre-appointment request must include all of the following:
      1) Pre-Appointment Check Request Memorandum.
      2) Completed security/suitability questionnaire. One of the following depending on the type of position:
         a) For Sensitive positions: Form SF-86, Questionnaire for National Security Positions, via e-QIP.
         b) For High-Risk and Moderate-Risk positions: Form SF-85P, Questionnaire for Public Trust Positions, via e-QIP.
         c) For Low-Risk positions: Form SF-85, Questionnaire for Non-Sensitive Positions, via e-QIP.
      3) Form SF-87, Fingerprint Chart, with OPM's designation in the "Operational Readiness Inspection (ORI) block.
      4) Form CD-79, Request for Security Clearance, with sufficient justification for access to the security level requested (for Sensitive positions only).
      5) Form OF-612, Optional Application for Federal Employment, or resume/equivalent.
      6) Form OF-306, Declaration for Federal Employment.
      7) Credit Release Authorization.
      8) Waiver Request (Critical Sensitive Positions Only).

d. **SSO Action**. The SSO shall review the pre-appointment check request package for completeness and forward a copy of the request package to OSY headquarters for action. OSY headquarters will perform the pre-appointment checks and notify the SHRM office of the results. The SHRM office will then notify OSY once the appointment date has been established.

2. **Waiver Request (*Critical Sensitive Positions Only*).** When a Critical Sensitive position appointment must be filled prior to the completion of an investigation because of an emergency situation, the individual's immediate supervisor must submit a waiver request memorandum with the request for a pre-appointment check. The waiver request memorandum shall be addressed to the Director.

   a. **Requirement.** The Director or his or her designee may grant a waiver of the requirement for prior completion of a SSBI for appointment to a Critical Sensitive position. The appointment must be justified as an emergency and in the national interest.
   b. **Procedure**. The individual's supervisor or unit manager will be responsible for initiating the request for a waiver and sending it through the SSO to OSY headquarters.
   c. **Request Package**. The SSBI request must include all of the following:
      1) The SSBI investigative request package coded for priority service request.
      2) Waiver request memorandum to OSY from the individual's supervisor or office manager, identifying the subject, the subject's proposed position sensitivity level, and the nature of the emergency and the national interest.
      3) Form SF-87, Fingerprint Chart, with OPM's designation in the ORI block.
      4) Credit Release Authorization.
   d. **SSO Action**. The SSO shall confirm that the waiver request memorandum clearly identifies the emergency need and the national interest and forward the waiver request package to OSY headquarters within three working days for processing.

3. **SAC** (Low Risk Contractors and Non-Federal Employees).

   a. **Requirement.** The SAC is the minimum investigative requirement for contract personnel and non-employees performing Low Risk functions.
   b. **Procedures.** The responsible Security Contact or Contracting Officer's Representative (COR) initiates the SAC request package. The Security Contact or the COR, not the subject, completes form OFI-86C, Items 1 through 12 and 14. The COR ensures that confirm code "R" is clearly written in Block 7 and that the subject has signed and dated Block 13, Authorization for Release of Information. The completed SAC request package is then sent to the SSO for processing no later than three working days after the subject's EOD.
   c. **Request Package.** The SAC request must include all of the following:
      1) Form OFI-86C, Special Agreement Checks.
      2) FD-258, Fingerprint Chart with OPM's designation in the ORI block.
   d. **SSO Action.** The SSO shall perform the following actions:

1) Review investigative request package for completeness.
2) Ensure that the subject of each package is identified as contract personnel, that the name of the contracting company or organization of origin is clearly indicated, and that each package is clearly marked to indicate the contract sensitivity designation.
3) Forward completed package to OPM.

4. **NACI (Low Risk Positions).**

a. **Requirement.** The NACI is the investigation requirement for appointment to a Low Risk position.
b. **Procedure.** The SHRM office sends the completed package to the SSO within three working days of the date the applicant certifies his or her e-Qip forms. COR will process contractor investigations through the SSO.
c. **Request Package.** The NACI request must include all of the following:
   1) e-QIP Signature pages from the SF-85, Questionnaire for Non-Sensitive Positions.
   2) Form OF-612, Optional Application for Federal Employment, or resume/equivalent.
   3) Form OF-306, Declaration for Federal Employment.
   4) Form SF-87 Fingerprint Chart, with OPM's designation in the ORI block (Federal Employees Only).
d. **SSO Action.** The SSO will review the completed NACI request and forward it to OPM for processing within three working days of the date the applicant certifies his or her e-QIP forms.

5. **ANACI (Non-critical Sensitive Positions).**

a. **Requirement.** The ANACI is the minimum initial investigative requirement for NCS positions requiring access to NSI up to the Secret level under E.O. 12968.
b. **Procedure.** The SHRM office provides the background investigative forms via e-QIP. The applicant or employee completes all forms, obtains a completed fingerprint card and set of fingerprints from the SSO (or local police station), and returns the completed investigative request package to the SSO for processing.
c. **Request Package.** The ANACI request must include all of the following:
   1) Pre-Appointment Check Request Memorandum.
   2) e-QIP Signature pages from the SF-86, Questionnaire for National Security Positions.
   3) Form OF-612, Optional Application for Federal Employment(federal employees only), or resume/equivalent (non-federal and federal employees).
   4) Form OF-306, Declaration for Federal Employment (federal employees only).
   5) Form SF-87, Fingerprint Chart, with OPM's designation in the ORI block.
   6) Form CD-79, Request for Security Clearance, with sufficient justification for access to the security level requested.
   7) Credit Release Authorization.

d. **SSO Action.** The SSO shall review the ANACI investigative request package for completeness and enter relevant data into OSY's electronic database. Upon favorably completed pre-appointment checks and subject's EOD date, the SSO shall send the ANACI request package to OPM for processing within three working days of the date the applicant certifies his or her e-QIP forms.

6. **NACLC (Non-Critical Sensitive contracts, non-federal employees, independent service contractors, Reinvestigation for Non-Critical Sensitive, and Moderate Risk Positions).**

   a. **Requirement.** The NACLC is the minimum investigation for contractor personnel, consultants, experts, associates, or committee members whose work requires access to NSI up to the Secret level.

   b. **Procedure.** The responsible Security Contact, COR, or Departmental committee liaison provides the NACLC forms to the individual via e-QIP prior to the start date or required date of association. The individual completes all forms, obtains a completed fingerprint card and set of fingerprints from the SSO (or local police station), and returns the completed investigative package to the Security Contact, COR, or Departmental committee liaison, who forwards the request package to the SSO for processing within three working days of the date the applicant certifies his or her e-QIP forms.

   c. **Request Package.** The NACLC request must include all of the following:
      1) e-QIP Signature pages from the SF-86, Questionnaire for National Security Positions.
      2) Form FD-258, Fingerprint chart, with OPM's designation in the ORI Block (Contractors and unpaid interns).
         Note: No fingerprint cards needed for reinvestigation.
      3) Form CD-79, Request for Security Clearance, with sufficient justification for access to NSI up to the Secret level.
      4) Credit Release Authorization.

   d. **SSO Action.** The SSO shall review the NACLC investigative request package for completeness, enter the relevant data into OSY's electronic database, and forward the request package to OPM for processing within three working days of the date the applicant certifies his or her e-QIP forms.

7. **CNACI (Child Care Worker).**

   a. **Requirement.** The CNACI meets the investigative requirements set forth by Public Law 101-647 and 42 U.S.C. § 13041 for individuals holding positions within childcare facilities. Employees of childcare facilities sponsored by the Department are subject to a CNACI conducted by OPM and will be reinvestigated every five years.

   b. **Procedure.**
      1) The Security Contact or the COR of the childcare contractor provides the CNACI investigative forms via e-QIP to the individual in advance of or on the

EOD date. The individual completes all forms, obtains a completed fingerprint card and set of fingerprints from the SSO (or local police station), and returns the completed investigative package to the Security Contact or COR, who forwards the request package to the SSO for processing within three working days of the date the applicant certifies his or her e-QIP forms.

2) The SSO reviews and submits the completed request package to OPM within three days of the individual's start of work.

c. **Request Package.** The CNACI request must include all of the following:
   1) e-QIP Signature pages from the SF-85, Questionnaire for Non-Sensitive Positions.
   2) Resume including professional qualifications and employment history.
   3) Form FD-258, Fingerprint Chart, with OPM's designation in the ORI block.
   4) Credit Release Authorization.

d. **SSO Action.** The SSO shall review the CNACI investigative request package for completeness and submit it to OPM for processing.

8. **MBI (Moderate Risk Positions).**

   a. **Requirement.** The MBI is the minimum investigation for appointment of employees to a Moderate-Risk position.

   b. **Procedure.** The SHRM office will forward the completed forms to OSY or the SSO office within three working days of the date the applicant certifies his or her e-Qip forms. COR will process contractor investigations through the SSO.

   c. **Request Package.** The MBI request must include all of the following:
      1) e-QIP Signature pages from the SF-85P, Questionnaire for Public Trust Positions.
      2) Form OF-612, Optional Application for Federal Employment, or resume/equivalent.
      3) Form OF-306, Declaration for Federal Employment.
      4) Form SF-87, Fingerprint Chart, with OPM's designation in the ORI block.
      5) Credit Release Authorization.

   d. **SSO Action.** None. The MBI request package will be reviewed by the SHRM offices for completeness and forwarded to the SSO within three working days of the date the applicant certifies his or her e-QIP forms.

9. **BI (High-Risk Positions).**

   a. **Requirement.**
      1) All employees and non-employees appointed to High Risk positions are subject to the completion of a BI prior to appointment.
      2) All appointments to High-Risk positions are subject to the prior completion of a BI; however, subjects can EOD after a pre-appointment check has been favorably completed.

   b. **Procedure.** The SHRM office initiates the individual into the OPM website to complete his or her security forms online with e-QIP, in advance of the EOD date.

The individual completes all forms, obtains a fingerprint card from the SSO (or local police station), and returns the signature pages from e-QIP and completed fingerprint card to the SHRM office. The SHRM office sends the completed package to the SSO for processing within three working days from the date the applicant certifies his or her e-QIP forms.

c. **Request Package.** The BI request must include all of the following:
   1) Pre-Appointment Check Request Memorandum.
   2) Waiver Request Memorandum, if required (refer to paragraph 11.5.B.).
   3) e-QIP Signature pages from the SF-85P, Questionnaire for Public Trust Positions.
   4) Form OF-612, Optional Application for Federal Employment, or resume/equivalent.
   5) Form OF-306, Declaration for Federal Employment.
   6) Fingerprint card. One of the following, depending on whether the person is a Government employee or a contractor/intern:
      a) Form SF-87, Fingerprint Chart, with OPM's designation in the ORI block (Federal Employees Only).
      b) Form FD-258, Fingerprint Chart, with OPM's designation in the ORI Block (contractors and unpaid interns).
   7) Credit Release Authorization.

d. **SSO Action**. The SSO shall review the BI request packages for completeness and forward the package to OSY for processing.

10. **SSBI (Special-Sensitive and Critical-Sensitive Positions).**

a. Requirement.
   1) All appointments to Special-Sensitive positions for employees requiring access to NSI at the Secret/Top Secret and SCI levels are subject to completion of an SSBI prior to appointment.
   2) All appointments to Critical-Sensitive positions for employees requiring access to NSI at the Top Secret level are subject to the prior completion of an SSBI.
   3) A pre-appointment check request memorandum is required for both Special-Sensitive and Critical-Sensitive positions.

b. **Procedure**. The SHRM office initiates the individual into the OPM website to complete his or her security forms online with e-QIP, in advance of the EOD date. The individual completes all forms, obtains a fingerprint card from the SSO (or local police station), and returns the signature pages from e-QIP and completed fingerprint card to the SHRM office. The SHRM office sends the completed package to the SSO for processing within three working days from the date the applicant certifies his or her e-QIP forms.

c. **Request Package**. The SSBI request must include all of the following:
   1) Pre-Appointment Checks Request Memorandum.

2) Waiver Request Memorandum *(Critical-Sensitive Only),* if required (refer to paragraph 11.5.B.2.
3) e-QIP Signature pages from the SF-86, Questionnaire for National Security Positions.
4) Form OF-612, Optional Application for Federal Employment, resume/equivalent, or personal qualifications statement.
5) Form OF-306, Declaration for Federal Employment.
6) Form SF-87, Fingerprint chart, with OPM's designation in the ORI block (Federal Employees Only).
7) Credit Release Authorization.
8) Form CD-516, Change of Position Designation (if needed).

d. **SSO Action**. The SSO shall review the SSBI request packages for completeness, enter relevant data into OSY's electronic database, and forward to OPM for processing. A copy of the completed package will be forwarded to OSY headquarters.

C. Re-investigations.

1. **NACLC (Non-Critical Sensitive Positions)..**

a. **Requirement**. All individuals occupying positions designated Non-Critical Sensitive are subject to a re-investigation at least once every 10 years. NACLC investigation is used for Non-Critical Sensitive position re-investigations, expiring MBIs, and initial NACLC investigations.
b. **Procedure.** The Security Contact or COR provides the re-investigation forms to the individual. The individual completes all forms and returns the completed investigative package to the SSO for processing. When completed, the SSO submits the re-investigation package to OPM for investigation with a copy provided to OSY headquarters.
c. **Request Package**. The re-investigation request must include all of the following:
1) e-QIP Signature pages from the SF-86, Questionnaire for National Security Positions.
2) Credit Release Authorization.
d. **SSO Action.** The SSO shall review the re-investigative request package for completeness and forward it to OPM.

2. **PRI (High-Risk Positions).**

a. **Requirement.** All individuals occupying positions High-Risk are subject to periodic re-investigation at least once every five years.
b. **Procedure**. The Security Contact initiates the individual's re-investigation forms via e-QIP. The individual completes all forms and returns the e-QIP signature pages to the SSO for processing. When completed the SSO submits the e-QIP signature pages to the SHRM, which, in turn, will submit the forms to OPM for investigation within three working days of the date the applicant certifies his or her e-QIP forms.

c. **Request Package.** The PRI request must include all of the following:
   1) e-QIP Signature pages from SF-85P, Questionnaire for Public Trust Positions. Forms must be updated by the subject with the top portion of the form completed by the Security Contact.
   2) Credit Release Authorization.

d. **SSO Action.** The Security Contact initiates the individual's re-investigation forms via e-QIP. The individual completes all forms and returns the e-QIP signature pages to the SSO for processing. When completed, the SSO submits the e-QIP signature pages to the Regional Security Office, which, in turn, will submit the forms to OPM for investigation within three working days of the date the applicant certifies his or her e-QIP forms.

3. **SSBI-PR (Special and Critical-Sensitive Positions with Secret/Top Secret Access).**

a. **Requirement.** All individuals occupying positions designated Special-Sensitive or Critical-Sensitive are subject to a reinvestigation at least once every five years.

b. **Procedure.** The Security Contact initiates the individual's SSBI-PR forms via e-QIP. The individual completes all forms and returns the e-QIP signature pages to the SSO for processing. When completed, the SSO submits the e-QIP signature pages to the Regional Security Office, which, in turn, will submit the forms to OPM for investigation within three working days from the date the applicant certifies his or her e-QIP forms.

c. **Request Package.** The SSBI-PR request must include all of the following:
   1) Form SF-86, Questionnaire for National Security Positions (Part I must be fully completed).
   2) Credit Release Authorization.

4. **SSO Action.** The SSO initiates the individual's SSBI-PR forms via e-QIP. The individual completes all forms and returns the e-QIP signature pages to the SSO for processing. When completed the SSO submits the forms to OPM for investigation within three working days from the date the applicant certified the e-QIP forms.

11.5. INVESTIGATIVE RESULTS

A. Initial Report of Investigation (ROI). After the personnel investigation has been completed, OPM or another investigative agency will forward the ROI to OSY. OSY will review the ROI only to determine the purpose for the investigation (e.g., upgrade of clearance for current employee, new security clearance, suitability on initial appointment) and will process the ROI as indicated below.

1. If the purpose of the investigation is to make a national security access eligibility determination only (e.g., upgrade of an existing clearance, a new clearance for a current employee already subjected to suitability investigation, a reinvestigation for security clearance renewal), OSY will review and adjudicate the ROI. After a final security decision has been made, OSY will update the adjudicative decision in the OPM Personnel Investigations Processing System (PIPS).

2. If the purpose of the investigation is for a suitability determination only (i.e., the position has no national security access requirements), OSY will forward the ROI to the SHRM office for appropriate action under the provisions of the DAO 202-731, Handbook on Suitability. The SHRM office will forward the INV-79A to OPM and a copy to OSY after a final suitability decision has been made.

B. Obtaining Supplemental Information.

1. OPM characterizes reports of investigation as either "no issues" or "with issues." When a suitability determination is necessary, investigations with "no issues" are normally certified as completed (same as a favorable adjudication) by the SHRM office without the need for additional information, suitability adjudication, or further action. Investigations "with issues" normally require additional information to clarify, enhance, refute, or otherwise mitigate or substantiate the limited information or "issues" found in the initial investigation. In addition, information may be needed from sources other than those identified in the initial investigation to clarify or confirm information that would mitigate or substantiate the issue or issues.
   a. If the additional information needed relates to law enforcement activities such as court documents, case disposition reports, and so forth, the SSO will assist the SHRM office in identifying, obtaining, interpreting, and analyzing the information.
   b. If the additional information needed is related to experience, conduct in previous employment, or education, the SHRM office, in collaboration with the cognizant management official, will identify, obtain, and analyze the information for either suitability or a national security investigation, or bot
2. Subject to the provisions of applicable statutes and executive directives, the subject of the investigation must be given an opportunity to explain or refute information obtained in the investigation or from additional sources prior to the agency's final adjudication for suitability and/or security purposes.

C. Actions Upon Final Adjudication.

1. Once suitability adjudication procedures have been followed, the SHRM office will follow the procedures outlined in DAO 202-731, Handbook on Suitability, including certifying the completion of the action, and/or notifying OPM of the results (in cases "with issues"), and notifying OPM of the results.
2. After the suitability process has been applied and the issues have been evaluated, if one or more serious issues remain that could potentially deny employment to an applicant, the SHRM office will take appropriate action and coordinate with OPM when applicable.
3. For national security investigations resulting in derogatory cases, OSY will take the lead in collaborating with the SHRM office on the final disposition of the case and the final action to be taken.

4. Possible actions resulting from unfavorable suitability/security adjudications include—

   a. Rejection of a selectee for the position.
   b. Acceptance and appointment of the selectee.
   c. Removal of the appointee or employee.
   d. Revocation or denial of the clearance.
   e. Reassignment of the appointee employee to a non-sensitive position.
   f. Retention of the appointee or employee coupled with appropriate disciplinary action.

5. Unfavorable suitability or security adjudications may be appealed for further review. Appeals of unfavorable suitability determinations only are described in DAO 202-731, Handbook on Suitability. Appeals for unfavorable security determinations are described in Chapter 14, Suspension, Downgrade, Revocation, and Denial of Access to NSI.

D. Personnel Security Records, Reporting, and Requests for Investigative Files.

1. **Records.** OSY maintains an electronic database record for each employee contractor, guest worker, research associate, or other individual associated with the Department. OSY will maintain security record information on a cleared individual for 5-years following the individual's association with the Department. Results of completed suitability determinations are filed in each employee's OPF. The SHRM office will provide copies of the INV-79A to OSY indicating the final suitability adjudication for suitability positions, and OSY will ensure OPM is provided the results of the adjudication via PIPS. The Personnel Security database will contain the results of adjudication determinations, including all of the following information:

   a. Name.
   b. Bureau.
   c. Position title (or other designation for non-employee).
   d. Date and place of birth.
   e. SSN.
   f. Position sensitivity/risk designation (Special Sensitive, Critical-Sensitive, Non-Critical Sensitive, High Risk, Moderate Risk, or Low Risk).
   g. Date of security briefings/debriefings.
   h. Access level (Top Secret, Secret), Special Access (e.g., DOE, NATO, SCI).
   i. Security processing action, including all of the following:
      1) Date initiated (sent to OSY or to OPM);
      2) Type of processing or security action (e.g., Pre-Appointment Checks, Personnel Investigation, Security Assurance, Security Access), including Department system of records;
      3) Date of completion and results for positions requiring a security determination; and
      4) EOD date and separation date.

2. **Reporting Personnel Actions.** The Security Contact shall report all appropriate personnel actions to OSY headquarters for inclusion in the Personnel Security database. The SSO is responsible for obtaining pertinent SF-50B (Notification of Personnel Action) information issued within his or her jurisdiction, and for forwarding to OSY those forms that indicate actions affecting, or possibly affecting, an individual's eligibility for security access. The following are examples of the types of personnel actions that may have a bearing on the Personnel Security Program. The list is not all-inclusive.

   a. Terminations for cause.
   b. Name changes.
   c. Changes in position sensitivity.
   d. Separations and transfers.
   e. Personnel transfers and reassignments.
   f. Suspensions and other disciplinary actions.
   g. Appointments.
   h. Details.
   i. Leave without pay in excess of 30 days.

3. **Requesting Personnel Security and Investigative Files.** OSY is the only repository for personnel security information in the Department. Accordingly, Privacy Act and FOIA requests for personnel security information will be referred to OSY for direct response to the requestor. However, reports of investigations to ROIs or other investigative agencies remain under the control of that agency; therefore, an individual will be required to submit his or her Privacy Act request to OPM or the appropriate agency to obtain a copy of the investigative file.

4. **Pending Security Processing.** The SSO or Security Contact will respond to requests for information concerning cases as requested by OSY headquarters.

E. Post Adjudication Reports

1. The FBI maintains fingerprint records for federal, military, and civilian employees. If the FBI receives criminal arrest fingerprints on a subject whose arrest record was previously released to OPM, a copy of the updated identification division record form (rap sheet) is also furnished to OPM. OPM reviews the information and determines if the individual is currently with a Federal agency. If so, OPM furnishes the rap sheet to the security office, designated by the Security Office Identifier (SOI), on the SF-85; SF-85P; or SF-86, along with a copy of a FIPC 402, "Agency Adjudication on FBI Post Appointment Arrest Form."

2. When OSY offices (headquarters or field) receive post arrest information, it is immediately forwarded to OSY or HR office responsible for the adjudication. The adjudicating office will review the new information along with existing investigation(s) to make a security/suitability determination, and forward the results to OPM on the FIPC 402. This process may require interviews with the subject.

3. Post arrest records for contractor employees may be shared with Contracting Officers to make continuing employment decisions.

Chapter 12. Access to Classified National Security Information

12.1. Granting Access to Classified National Security Information

This chapter covers investigative processing procedures and requirements associated with granting eligibility for access to Classified National Security Information (NSI), also known as a security clearance. The granting of eligibility for access to NSI is an administrative decision and is used only when access is clearly consistent with the interests of national security. Final access to NSI is based on a favorably adjudicated background investigation, security indoctrination, an executed Classified Information Nondisclosure Agreement (SF-312), and/or a Sensitive Compartmented Information Nondisclosure Agreement (Form-4414), and a need to know. The Director for Security (Director) delegates to the Assistant Director for Counterespionage, the authority to grant a security clearance upon determining that the individual is trustworthy and free from unacceptable risk concerning the protection of NSI. Security clearances within the Department of Commerce (Department) are issued at the Top Secret and Secret levels. Individuals requiring access to Confidential information will be granted a clearance at the Secret level. The need to know is established by management officials based on the official duties of the position that the employee holds.

A. Eligibility for Access to NSI.

1. A security clearance is an indication that a determination of trustworthiness has been made and has been granted in accordance with Executive Order (E.O.) 12968, Access to Classified Information, and E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information. A need for access to NSI must be demonstrated before a request for a security clearance can be initiated. The number of people cleared and granted access to NSI should be maintained at the minimum number that is consistent with operational requirements and needs. Heads of operating units must ensure that access to NSI by unauthorized persons is prevented.

2. No one has a right to gain access to NSI solely by virtue of title, position, or level of security clearance. The final responsibility for determining whether an individual requires access to NSI and whether the individual has been granted the appropriate security clearance rests with the individual who has possession, knowledge, or control of the information and not with the prospective recipient. The fact that an individual is a federal employee does not mean that he or she has been cleared for access to NSI. The need for disclosure of NSI to the recipient and the recipient's identification and security clearance shall be verified by the Servicing Security Office (SSO). The individual holding or controlling NSI shall advise the recipient of the classification level of the information.

3. When an employee transfers or vacates a position, his need to know changes. Security clearances do not transfer with the employee. In such cases, the need to know must be reestablished and a new request submitted to the employee's SSO with appropriate

justification before a new clearance is granted. Depending on circumstances, the existing investigation may be used as the basis for issuing the new clearance.

B. Determining Eligibility for Access to NSI.

1. The procedures for requesting personnel security investigations for the purpose of making a security clearance determination are listed in Chapter 11, Investigative Processing.

2. A person's eligibility for a security clearance and access to NSI are based on the following criteria.
   a. **Eligibility.** The individual is found loyal, trustworthy, and free from unacceptable risks, based upon an appropriate background investigation and the appropriate sensitivity level.
   b. **Access.** The access to NSI is essential to accomplish a lawful and authorized Government purpose (need to know) and the individual has entered into an agreement with the Federal Government to protect NSI and to prevent unauthorized disclosure. The SF- 312 shall be used for employees and non-employees.

3. The decision to grant eligibility for access to NSI must be fair, impartial, and based on a consideration of all available information. Therefore, the Adjudication Guidelines for Determining Eligibility for Access to Classified Information in Chapter 13 will be used to adjudicate all NSI cases. The review of adverse information shall include, but is not limited to, consideration of the following factors.
   a. Nature and seriousness of the facts, circumstances, or conduct.
   b. Circumstances surrounding the conduct.
   c. Frequency and recentness of the conduct.
   d. Age of the individual at the time of the incident.
   e. Motivation of the individual, or the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the circumstances or consequences involved.
   f. Absence or presence of positive evidence of rehabilitation.
   g. Probability that the facts, conduct, or circumstances, to the extent that it can be estimated, will or will not continue or recur in the future.

4. The following general requirements apply to the process of determining eligibility for access to NSI.
   a. Naturalized citizens may be considered for access eligibility in the same manner as native-born U.S. citizens.
   b. Foreign nationals generally are not eligible for a security clearance. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to NSI. However, compelling reasons may exist to grant access to NSI to an immigrant alien or a foreign national. Such individuals may be granted a Limited Access Authorization in those rare circumstances where the non-U.S. citizen possesses unique or unusual skill or expertise that is urgently needed to

support a specific U.S. Government project involving access to specified NSI and a cleared or clearable U.S. citizen is not readily available.

c. Non-Employees/Contractors may be granted a security clearance under the National Industrial Security Program. On a case-by-case basis, the Office of Security (OSY) may grant individual contractors a security clearance for the performance of short-term classified work. Information on processing this request is contained in Chapter 37.

d. Non-employees other than contractors generally will not be provided access to NSI. Some exceptions exist for those non-employees being processed for membership on a Departmental advisory committee that requires access to NSI.

C. Exceptions. Within the limits of administrative discretion permitted by the Department, exceptions to the provisions of this paragraph may be granted by the Director, or his or her designated representative, whenever such an exception would be in the interest of the national security and would promote the efficiency of the service. Each request for such an exception shall be submitted in writing and shall contain a statement justifying the request.

12.2. REQUESTING A SECURITY CLEARANCE

A. Request Forms. The immediate supervisor or program manager must request and justify a security clearance for a subordinate employee. The request must be forwarded to the SSO. The form CD-79, Request for Security Clearance, shall be used to request a security clearance. The individual must also have the proper Position (Sensitivity) designation. If the individual is listed as a Risk Designation, then no clearance will be granted until the supervisor or program manager provides a stamped copy of CD-516, Classification and Performance Management Record and a screen shot of the National Finance Center record showing the position designation has been changed by the Servicing Human Resources Management (SHRM) office. Incomplete packages will be returned through the SSO to the operating unit for appropriate action.

1. The CD-79 must state the requested level of clearance (Top Secret or Secret) and must justify the need for access. The request must describe the individual's need to know, the nature of access, how often it will occur, and the duration required for the clearance. If the duration is for the time the individual encumbers the current position, it must be so stated. The SSO must concur by signing the concurrence block on the CD-79.

2. The SF-86, Questionnaire for National Security Positions, provides current biographical information to establish eligibility for access. A new or an updated SF-86 may be required when OSY does not have one on file.

3. Access to NSI is not permissible until the SF-312 is signed, but only after the individual has received an NSI briefing and the approving authority has granted eligibility for access to NSI; therefore, the SF-312 will not be sent with the clearance request. The SF-312 is a legally binding document that grants the signer access to NSI upon signature, in return for abiding by its requirements.

4. Detailed Overview for Processing Normal Eligibility for Access to NSI.
   a. **Requirements.** All requests for access (Top Secret or Secret) shall be granted based on a need to know; a justification for access; proper investigation, initial security education and awareness briefing; and a signed SF-312, (after a formal NSI briefing). A Single Scope Background Investigation (SSBI) is required for Top Secret/SCI access in Special Sensitive positions, for Top Secret clearance in a Critical Sensitive position, and for Secret clearance in a Critical Sensitive position; the Access National Agency Check with Inquiries (ANACI) is the minimum investigation for a Secret clearance in a Non-Critical Sensitive position.
   b. **Procedures.** An individual's supervisor initiates a request for access and forwards it to the operating unit's SSO, who reviews it for completeness and sends it to OSY Counterespionage Division (CED).
   c. Required Documents.
      1) Signature pages from the e-QIP SF-86, Questionnaire for National Security Positions.
      2) Form CD-79, Request for Security Clearance.
      3) Credit Release Authorization (included in signature pages from the SF-86).
      4) CAS fingerprint results.
      5) Resume.
   d. SSO Actions.
      1) Enter all pertinent information into the OSY database (Security Manager).
      2) Review the documents for completeness.
      3) Confirm the subject has an appropriate need to know.
      4) Confirm the justification for level of security access requested on Form CD-79, Request for Security Clearance.
      5) Confirm the SF-86 is signed, certified within three calendar days of the applicant's certification and released to the SSO, and not more than 10 calendar days prior to submission to the Office of Personnel Management (OPM).
      6) Confirm that the block labeled "Primary Unit" on the CD-79 identifies the operating unit, agency, and SSO (if needed) initiating the request.
      7) Forward the request for eligibility for access to OSY CED.
      8) Upon receipt of favorable eligibility for access determination from OSY headquarters, the SSO will conduct an initial security education and awareness briefing.
      9) Instruct the subject to read and sign the SF-312, and obtain a third individual's witness signature.
      10) Forward the SF-312 to OSY CED to document clearance in the Security Manager database.

B. Interim Eligibility for Access.

1. Based on exceptional circumstances meeting the requirements of E.O. 12968 and E.O. 13467, interim eligibility for access to NSI may be granted before investigations

are complete and favorably adjudicated if official functions must be performed prior to completion of the investigation and adjudication process as long as a favorable pre-appointment determination has been made by OSY's submission of the appropriate background investigation. The interim eligibility will be valid until completion of the investigation and adjudication; however, the Department may revoke the access at any time based on unfavorable information developed in the course of the investigation. When such eligibility is granted, the initial investigation shall be expedited.

2. Interim eligibility for access must be requested by memorandum to OSY. The justification for the access must be indicated on the CD-79, Request for Security Clearance. The Director, or his or her designee, may grant interim eligibility for access when an emergency need exists. Interim eligibility allows access to NSI under controlled circumstances when the basis for granting a final security clearance has not been completed.

   Note: Interim eligibility for access is not always reciprocal with other departments or agencies.

C. Temporary Access to NSI.

1. When an employee does not normally require access to NSI as a part of his or her routine duties, eligibility for access may be granted on a temporary basis when required for special meetings, conferences, projects, or other one-time, non-routine events. Such temporary access can be granted only if the employee has been determined to be eligible for access to NSI based on a favorably adjudicated background investigation, has executed a nondisclosure agreement and received a security indoctrination, and the employee's supervisor has submitted a CD-79 justifying the need for the temporary access. Access to NSI shall be terminated when an employee no longer has a need for access.

2. When the access granted under this paragraph involves another agency's NSI, that agency must concur before access to its information is granted.

3. Detailed Overview for Processing Temporary Eligibility for Access to NSI.
   a. **Requirement.** Temporary eligibility for access to NSI requests may be granted by the Director, or his designee, if an emergency need exists. Temporary eligibility for access allows an individual to have access to NSI for a specified period of time. Temporary eligibility for access may be granted only with a clearly demonstrated emergency requirement and need to know; a background investigation submitted to OPM with a 35-day service request (when a higher level of clearance is required); a signed SF-312, an initial security education and awareness briefing; and a favorable Pre-Appointment Check.
   b. **Procedure.** The subject's management office initiates the request for temporary eligibility for access to NSI, reviews it for completeness and sends it to the SSO.
   c. **Required Documents (When subject does not have a current investigation to support the temporary clearance).**

1) Temporary eligibility for access request memorandum to the Director.
2) CD-79, including a paragraph with specific and detailed justification for the request for temporary eligibility for access.
3) Signature pages from e-QIP for SF-86.
4) Credit Release Authorization (included in signature pages from the SF-86).
5) Fingerprints.
6) Resume.

d. **SSO Actions.**

1) Review the temporary access required documents for completeness.
2) Confirm the subject has an appropriate need to know.
3) Confirm justification for level of security access is shown on CD-79.
4) Confirm SF-86, is signed within three calendar days of the applicant's certification, and release to the SSO, and not more than 10 calendar days prior to submission to OPM.
5) Confirm that the block labeled "Primary Unit" on the CD-79 identifies the operating unit initiating the request.
6) Forward the request for temporary eligibility for access to OSY headquarters.
7) Upon receipt of favorable eligibility for access determination from OSY CED, conduct an initial security education and awareness briefing.
8) Instruct the subject to read and sign the SF-312, and obtain a third individual's witness signature.
9) Enter all pertinent data into OSY's Security Manager database.
10) Forward the SF-312 to OSY CED, which will grant eligibility for access to NSI upon receipt.

12.3. ADMINISTRATIVE DOWNGRADE OR TERMINATION OF SECURITY CLEARANCE

A security clearance may be downgraded or terminated for administrative reasons unrelated to an adverse security determination. Just as the immediate supervisor or program manager is responsible for requesting a security clearance, he or she is also responsible for advising the SSO whenever administrative downgrade or termination of security clearance is appropriate based on changed need to know. Whenever there is an administrative action, the individual must be advised of the action. The administrative downgrade or termination of an individual's security clearance does not prejudice the person's eligibility for a future security clearance. Administrative action is required in the examples to follow. In each case of termination or downgrade of access to NSI, the SSO shall notify the SHRM office so that the position records can be updated.

A. When access to the Top Secret level of NSI is no longer required in the performance of official duties the clearance must be downgraded to the Secret level, and still justified by official duties. To initiate a downgrade action, the immediate supervisor must forward a CD-79, Request for Security Clearance, justifying the new clearance level indicating, "Administrative Downgrade" in the "Justification" block of the form, and stating that the employee has been notified of the downgrade action.

B. When access to a particular level of NSI is no longer required in the performance of official duties, the clearance must be downgraded to a classification level still justified by official duties. To initiate a downgrade action, the immediate supervisor must forward a CD-79, justifying the new clearance level indicating, "Administrative Downgrade" in the "Justification" block of the form, and stating that the employee has been notified of the downgrade action.

C. Upon termination of a security clearance, the holder must receive a formal security debriefing describing the continuing responsibility to protect the NSI to which the individual had access. The debriefing portion of the SF-312 shall be completed.

D. When the supervisor and/or SHRM office downgrades an individual's position sensitivity to a risk level, the clearance will be administratively withdrawn. The debriefing portion of the SF-312 shall be completed upon debriefing.

E. NSI (in any form), including extra copies, is not personal property and may not be removed from the Federal Government's control by any departing official. The Security Contact must ensure that all debriefed personnel have turned over all NSI in their possession and ensure that all NSI is accounted for upon transfer to an authorized custodian. All departing personnel must be debriefed and understand their ongoing security responsibilities in protecting NSI to which they had access.

12.4. SUSPENSION AND REVOCATION OF ACCESS ELIGIBILITY FOR CAUSE

A. Whenever information is received that indicates an employee's continued access to NSI is not in the interests of national security, such information shall be forwarded immediately to OSY CED. Guidelines for standards of conduct related to security determinations are set forth in Chapter 13, Security Adjudication Criteria.

B. Whenever the SHRM office obtains information that suggests continuation of an individual's security clearance is not in the best interest of national security, he or she may suspend the individual's security clearance pending an investigation to resolve the issues.

C. Accordingly, whenever an investigation develops information that confirms an individual's disloyalty to the country or untrustworthiness, or raises issues of unacceptable security risk, the Assistant Director for Counterespionage will issue a proposal to revoke or downgrade an individual's security clearance, as appropriate. Such security determinations for cause will be made independently of a suitability determination conducted by the servicing human resources manager.

D. The servicing human resources manager and SSO will be advised of all security clearance actions for cause. When an individual's security clearance has been suspended, the SSO must notify the immediate supervisor or program manager to ensure that appropriate action is taken in connection with the individual's access to NSI.

E. The procedures described in Chapter 14, Suspension, Downgrade, Revocation, and Denial of Access to Classified National Security Information, shall be followed by OSY when conducting a formal review to determine an individual's continued eligibility for access to NSI based on unfavorable information that may lead to the denial, downgrade, or revocation of that clearance.

F. When misconduct is reported to the SHRM office and the individual occupies a sensitive position, the servicing human resources specialist shall contact the SSO immediately. The investigation of the misconduct must be coordinated, and normally the national security interest will be investigated first.

G. The results of the investigations are shared between the security and human resources offices. The Office of General Counsel shall be included in the deliberative process to decide what action(s) to take.

12.5. TRANSMITTING SECURITY ACCESS INFORMATION

A. Visit Authorization and Security Clearance Certification Request.

1. **Visits to Other Government Agencies Requiring SCI Clearance.** Only OSY CED and the SSO can certify and transmit SCI clearances to other Government agencies. The Security Contact shall provide the following information to the CED/SSO at least five working days in advance of the proposed visit. The CED/SSO will forward the submitted information to the CIA at least three working days in advance of the proposed visit.
   a. Requestor's name and telephone number.
   b. Visitor's name, date, place of birth, and Social Security number (SSN).
   c. Security clearance required.
   d. Site of visit: name and location of the agency to be visited.
   e. Date range of the proposed visit.
   f. Name and telephone number of the point of contact for the project/program associated with the visit.
   g. Purpose of visit: unclassified description.
2. **Visits to Other Government Agencies *not* Requiring SCI Clearance.** The SSO may certify an employee's security clearance to other Government agencies after verifying such status in OSY database. The CD-414, Visit Authorization and Security Clearance Certification Request, will be used for this purpose. The Security Contact will complete the following items of the form.
   a. Item 1: Name of contact to be visited, organization, address, and telephone number.
   b. Item 2: Visitor's name, organization, address, and telephone number.
   c. Item 3: Visitor's name and SSN.
   d. Item 5: Purpose of visit.
   e. Item 6: Dates of visit.
   f. Item 8: Security points of contact, name, organization, address, and telephone number.

g. Item 9: Remarks.
h. Item 10: Requestor's organization and date of request.
i. Item 11: Need-to-Know Certification.

3. **Visits to a Department Operating Unit in Another SSO's Jurisdiction**. The SSO may pass security clearance information directly to the SSO of another jurisdiction within which the visit will take place. Such certification will use the CD-414 for this purpose. The Security Contact or SSO will complete the same items as outlined in 2 above.

4. **Visits to a Department Office Within the SSO's Jurisdiction**. The SSO is responsible for confirming security access information to the head of the office to be visited with the CD-414.

B. Personnel Transfers.

1. **Within a Department Operating Unit But Between SSO Jurisdictions.** The relinquishing SSO shall forward, in a timely manner, a copy of the employee's Security Index record to the gaining SSO. The gaining SSO will be responsible for incorporating the security record information into his or her Security Index and advising OSY in writing of the change in jurisdiction and any change in position title, position sensitivity, and/or level of security clearance needed. The receiving SSO must process upgrades or downgrades of security clearance.

2. **To Another Government Agency**. The Security Contact is responsible for notifying the SSO of all such transfers. However, OSY will handle agency requests for security clearance information, processing basis, and security file review. All such inquiries received by the SSO shall be directed to OSY.

3. **To Different Department Operating Units Within the Same SSO's Jurisdiction.** The SSO is responsible for informing OSY, in writing, of the employee's new operating unit, position title, change in position sensitivity, and new security clearance needs, if any.

4. **To Different Department Operating Units Between SSOs**. The relinquishing SSO's responsibilities will be the same as those shown in paragraph B.2 above. The gaining SSO's responsibilities will also remain the same as paragraph B.2 above with the added responsibility of advising OSY, in writing, of the employee's new operating unit.

5. **Security Clearance Does Not Automatically Transfer with the Individual.** Any permanent change in operating unit, or even a significant change of duties within the same operating unit, requires that the security clearance be requested justified by means of CD-79. This is true even if the level of clearance remains the same.

Chapter 13. Adjudication Criteria

13.1. ADJUDICATION DETERMINATIONS

The criteria set forth in this chapter are used to support two separate, but related, national security adjudication determinations. One is the adjudication of investigative information to determine suitability for employment; the other is adjudication to determine a person's eligibility for access to Classified National Security Information (NSI).

13.2. NATIONAL SECURITY DETERMINATIONS

A. No person shall be employed or retained in the Department unless the employment of such a person is clearly consistent with the national security and/or the efficiency of the service.

B. No person shall be granted eligibility for access to NSI or retain access unless such access is clearly consistent with the national security.

C. National security adjudication determines an individual's eligibility to be granted national security access as described in Chapter 12, Access to Classified National Security Information. Appointment to or retention in employment is a separate determination relating to the overall risk to the national security and efficiency of the federal service. An unfavorable national security adjudication may result in a negative employment determination when a selectee is being considered for a position that requires NSI access. In the case of a current employee, however, the servicing human resources management office requires a separate retention decision.

13.3. CRITERIA FOR MAKING DETERMINATIONS

The criteria for determining suitability for employment or eligibility for access to NSI under the national security standard shall include, but not be limited to, the following:

A. The following guidelines are considered as a basis for suitability under 5 CFR 731:

1. Misconduct or negligence in employment;
2. Criminal or dishonest conduct;
3. Material, intentional false statement, deception or fraud in examination or appointment;
4. Refusal to furnish testimony as required by §5.4 of this title;
5. Alcohol abuse of a nature and duration which suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of others;
6. Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;
7. Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government for force;

8. Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

B. The following guidelines are for access to NSI:

1. Guideline A: Allegiance to the United States
2. Guideline B: Foreign Influence
3. Guideline C: Foreign Preference
4. Guideline D: Sexual Behavior
5. Guideline E: Personal Conduct
6. Guideline F: Financial Considerations
7. Guideline G: Alcohol Consumption
8. Guideline H: Drug Involvement
9. Guideline I: Psychological Conditions
10. Guideline J: Criminal Conduct
11. Guideline K: Handling Protected Information
12. Guideline L: Outside Activities
13. Guideline M: Use of Information Technology Systems

Chapter 14. Suspension, Downgrade, Revocation, and Denial of Access to Classified National Security Information

14.1. Access to Classified National Security Information

Access to Classified National Security Information (NSI) is a privilege that must be taken very seriously and guarded very closely. Whenever there is a potential threat or risk to national security, the Department of Commerce (Department) must evaluate the risk and make a decision based on all the facts available. Security officials in the Department, however, will carefully review all information presented by an applicant, employee, or other person associated with the Department, or the individual's representative on his or her behalf, and arrive at a fully validated and supported decision regarding access to NSI, based on all appropriate laws and regulations.

14.2. Derogatory Information

A. Whenever information related to Chapter 13, Security Adjudication Criteria, indicates that access to NSI by an employee or other person associated with the Department is not in the interest of national security, the supervisor, manager, or other employee of the Department shall forward that information immediately in writing through the Servicing Security Office (SSO) to the Personnel Security Branch of the Counterespionage Division (CED).

B. The information will be promptly evaluated to determine the individual's eligibility or continued eligibility for access to NSI. The information may also require evaluation for fitness for employment. If the information contained in the report is insufficient to make a determination, the Assistant Director, CED may conduct or request an additional investigation, as necessary, to reach a decision concerning the impact on national security. During the inquiry, all reasonable efforts must be expended to develop the facts and circumstances to resolve pertinent security issues. The Assistant Director's determination will be made in writing and will be made a part of the investigative file.

C. Derogatory information, which may be obtained through a variety of sources and at various times during selection, appointment, and employment, shall be evaluated from both an employment and a national security perspective. Reports of investigation from investigative agencies and information concerning security issues shall be provided to the Personnel Security Branch of CED. Derogatory information concerning employment and reports of employee misconduct are typically provided to the Servicing Human Resources Management (SHRM) office.

D. Additional derogatory information obtained during the investigation will be shared between the CED and the SHRM office. The national security decision typically will be made prior to any employment or disciplinary decision. The CED, SHRM office, and Office of General Counsel (OGC) will consult to determine the best course of action based on the facts obtained during the investigation.

14.3. SUSPENSION OF ACCESS TO NSI

A. In this chapter, the term "employee" shall include civil service employees, contract employees, and experts and consultants who have been granted access to NSI by the Department.

B. Whenever CED becomes aware of information which suggests continuation of an individual's security clearance is not in the interest of national security, the employee's eligibility for access may be immediately suspended, pending an investigation to resolve the issue(s). The review and appeal procedures set forth in the following paragraphs do not apply to the suspension of an employee's access to NSI but only to the proposal to revoke, downgrade, or deny eligibility for that access. A suspension of an employee's eligibility for access to NSI will not be indefinite. It will be reviewed every 30 days by the Personnel Security Branch in consultation with the Assistant Director, CED.

C. Factors to consider in making a determination to suspend an employee's access to NSI shall include all of the following:

1. The seriousness of the derogatory information developed.
2. The possible access of the employee, whether authorized or unauthorized, to NSI.
3. The opportunity, by reason of the nature of the position, for committing acts that can adversely affect national security.

D. Pending a determination by the Assistant Director, CED, the employee may be detailed temporarily to a position that does not require a security clearance.

E. Written notification of the clearance suspension will be provided to the SSO.

F. Upon favorable completion of the investigation the supervisor must submit a written request to reinstate the employee's security clearance.

14.4. PROCEDURES TO REVOKE, DOWNGRADE, OR DENY ELIGIBILITY FOR ACCESS

A. When an investigation or inquiry provides information that confirms an applicant's or employee's disloyalty to the country or untrustworthiness, or raises issues of unacceptable security risk, the Assistant Director, CED may rescind, downgrade, or place restrictions on an individual's security clearance, as appropriate. Such clearance determinations for cause will be made subsequent to the suitability determination of the SHRM office. The Assistant Director, CED will advise the servicing SHRM office of all security clearance actions for cause, notify the immediate supervisor or manager, and ensure that appropriate action is taken in connection with the individual's access to NSI.

B. Subject to restrictions on disclosure of NSI, an individual whose eligibility for access has been revoked, downgraded, or denied for cause shall have an opportunity to explain or to refute derogatory information developed in an investigation before such action is finalized based on the procedures outlined in the following paragraphs. The purpose of this provision is to prevent errors that might otherwise result from mistakes in identity or

from mitigating circumstances that are unknown to the Office of Security (OSY). This provision does not apply to the suspension of a security clearance pending the completion of an investigation.

C. If the Assistant Director, CED makes a determination that granting eligibility for access to NSI to an applicant or employee remains an unacceptable security risk, a proposal will be issued to revoke, downgrade, or deny the applicant's or employee's eligibility for access. Such proposals will be made in accordance with the procedures outlined below. A suitability determination conducted by the SHRM office concerning employment in the Department will be made independently of the proposal to revoke, downgrade, or deny an applicant or employee's eligibility for access to NSI. The SHRM office will make the suitability determination after the final denial has been upheld by the Director for Security (Director).

D. An applicant or employee whose access to NSI has been revoked, downgraded, or denied shall be provided with all of the following if requested:

1. A comprehensive and detailed written explanation of the basis for that conclusion as permitted by the national security interests of the United States and other applicable laws.
2. Any document, record, and/or report upon which the proposal is based, as permitted by the national security and other applicable laws.
3. A reasonable opportunity to reply in writing to the Assistant Director, CED and to request a review of the information from which the proposal to revoke, downgrade, or deny eligibility for access was made.
4. The right to be represented by counsel or other representative at his or her own expense, for an appeal to the Deputy Director for Security (Deputy Director).
5. An opportunity to appear personally before an Access Review Panel (ARP), with or without representation, to give an oral response and present relevant documents, materials, and information that would explain, mitigate, or clarify the security issues concerning the proposal to revoke, downgrade, or deny eligibility for access to NSI.

E. In carrying out the provisions of this chapter, applicable regulations pertaining to the safeguarding of NSI and the handling of investigative reports shall be strictly enforced. No NSI, nor any information that might compromise investigative sources or methods or the identity of confidential informants, shall be disclosed to any employee, his or her counsel or representative, or any other person not clearly authorized access to such information.

14.5. REQUEST FOR SECURITY AND INVESTIGATIVE FILES

A. An applicant or employee who requests relevant information in his or her personnel security file and/or report of investigation shall be provided all releasable documents, records, and/or reports within 30 calendar days of the Department's receipt of the request, provided that the documents, records, and/or reports are the exclusive records of

the Department, and that they are releasable under laws pertaining to national security, privacy, freedom of information, and/or other pertinent regulations. The applicant or employee must request the security file and/or report of investigation in accordance with procedures under the Privacy Act,): http://www.archives.gov/about/laws/privacy-act-1974.html and within 14 calendar days of receipt of the proposal to revoke, downgrade, or deny eligibility for access. Requests under the Privacy Act for documents, records, and reports contained in the Department's Personnel Security file shall be sent to the following address:

U.S. Department of Commerce
Office of Security, Room 1067
ATTN: Privacy Act Request
1401 Constitution Ave., NW
Washington, DC 20230

B. If the proposal to revoke, downgrade, or deny an applicant's or employee's eligibility for access to NSI was based on an investigation by a non-Department investigative agency, the applicant or employee will be required to request the Report of Investigation (ROI) directly from the investigative agency within 14 calendar days of receipt of the proposal and in accordance with Privacy Act procedures. A copy of the request to the non-Department investigative agency must also be forwarded to OSY.

1. The Office of Personnel Management (OPM) generally conducts personnel security investigations for the Department. Requests for reports of investigations (ROI) conducted by OPM must be sent as a Privacy Act request to the following address:

   FOI/P, OPM-FIPC
   1137 Branchton Road
   Boyers, PA 16018-0618

2. If the ROI was conducted by another investigative agency, the Department will provide the appropriate address to the employee or applicant.

C. Upon notification that an individual has requested relevant information in his or her personnel security file, OSY will grant a reasonable amount of time for the individual to receive the information and provide a written response to the Assistant Director, CED. The requester will be presumed to have received documents requested from an outside investigative agency within 30 calendar days of the date of the request for such documents unless he or she notifies the Assistant Director, CED and requests additional time to prepare his or her response.

14.6. REQUEST TO REVIEW PROPOSED REVOCATION OF ACCESS

A. Individuals have the right to reply to the proposal to revoke, downgrade, or deny eligibility for access to NSI orally, in writing, or both, and to present information that would explain or clarify the security issues concerning the revocation, downgrade, or denial proposal. Upon receipt of the relevant information in the personnel security file

from OSY, the ROI from the appropriate investigative agency, or a notice of non-availability or denial of documents from either source, the applicant or employee shall have 14 calendar days to reply in writing to explain the issues and/or request a review by the Deputy Director regarding the proposal to revoke, downgrade, or deny eligibility for access to NSI.

B. If OSY does not receive a request for review of the proposed revocation, downgrade, or denial of an individual's eligibility for access to NSI or does not receive a copy of the request for the individual's personnel security file or the report of investigation within 14 calendar days of receipt of the initial notice, the Deputy Director will issue a final decision to the individual revoking, downgrading, or denying their eligibility for access to NSI. A copy of this decision will be forwarded to an employee's supervisor for appropriate action.

14.7. APPEAL TO THE ARP

A. If the Director makes a decision to sustain the revocation, downgrade, or denial proposal, the individual shall be:

1. Provided written notice of the decision and the reasons, the identity of the deciding official, and the right to appeal the decision to an ARP, regardless of whether or not a reply to the proposal was made.
2. Given 30 calendar days from receipt of the notification to provide a written reply to the ARP established by the Director, or designee.
3. Given the opportunity to appear personally, with or without a representative, before the ARP and present relevant documents, materials, or information that would explain or clarify the security issues concerning the revocation, downgrade, or denial decision. A written record of any oral reply shall be prepared by OSY and maintained in the individual's personnel security file. A copy of this report shall be provided to the individual.

B. If an applicant or employee appeals the decision to revoke, downgrade, or deny their eligibility for access to NSI, the Director, or designee, shall establish an ARP to review the appeal.

1. The ARP shall consist of three senior Federal Government employees who are cleared to at least the Secret level (or Top Secret, if needed for the particular case). Each panel member shall be at a grade level equal to or higher than the applicant/employee. Two of the panel members shall be selected from outside of the security field, one of which will be a representative of the operating unit to which the employee is assigned.
2. The Director, or designee, shall appoint members to the ARP.
3. OSY shall provide administrative and technical support to the ARP.

C. The ARP shall convene to review the Deputy Director's decision to revoke, downgrade, or deny an individual's eligibility for access to NSI and to consider the appeal by the individual to overturn this decision. The ARP shall review all pertinent documents, records, files, inquiries, and investigations to determine the validity of the revocation, downgrade, or denial decision and to sustain or reverse the Deputy Director's decision. Decisions of the panel shall be conveyed in writing and considered final unless reviewed and reversed by the Secretary of Commerce (Secretary) as indicated below.

14.8. REVIEW BY THE SECRETARY

A. The Director shall review the proceedings of the ARP and determine whether the record of the proceedings should be forwarded to the Secretary (or his or her designee) for review.

B. Nothing in this process shall prohibit the Secretary (or his or her designee) from personally exercising his or her authority to review the appeal of an applicant or employee and the decision of the ARP. In such cases, the decision of the Secretary shall be final. The review by the Secretary is not at the discretion of the person who was denied access eligibility or whose eligibility was downgraded or revoked but shall be determined solely by the Director.

14.9. FOLLOW-UP AND CORRECTIVE ACTION

A. The SSO and SHRM office shall be notified immediately of any decision to suspend, downgrade, deny, or revoke an individual's eligibility for access to NSI. For employees, a copy of this decision shall be sent to the individual's supervisor. The SSO shall provide support and assistance to the individual's supervisor or program manager to ensure that appropriate action is taken to restrict the individual's access to NSI.

B. Nothing in this chapter shall limit or affect the responsibility and authority of an operating unit or Departmental office in making determinations of suitability for employment when an employee's eligibility for access to NSI has been revoked. The SSO, the Assistant Director, CED, or designee, may be consulted by the SHRM office to ensure understanding of the seriousness of any security incident or violation that leads to the decision to revoke or downgrade eligibility for access to NSI. Such a review may include describing the potential for or extent of damage to national security. The SHRM office will consult with the OGC, as appropriate.

14.10. SAFEGUARDING NSI

A. In carrying out the provisions of this policy, applicable regulations pertaining to the safeguarding of NSI and the handling of investigative reports shall be strictly enforced. No NSI, nor any information that might compromise investigative sources or methods or the identity of confidential informants, shall be disclosed to any individual, to his or her counsel or representative, or to any other person not clearly authorized access to such information.

B. When the Secretary or Deputy Secretary (or designee) makes a decision based on recommendations of the Director that a procedure set forth in this Manual of Security Policies and Procedures cannot occur in a particular case without damaging the national security interests of the United States by revealing NSI, the particular procedure shall not occur. The certification by the Secretary or Deputy Secretary shall be conclusive and final.

14.11. EXCEPTIONS

A. Nothing in this chapter shall limit or affect the responsibility and power of the Secretary to carry out any law or other Executive Order (E.O.) to deny or terminate an employee's eligibility for access to classified NSI in the interests of national security. The power and responsibility to deny or terminate access to NSI pursuant to any law or other E.O. may be exercised only when the Secretary or Deputy Secretary determines that the procedures prescribed in this manual cannot be invoked in a manner that is consistent with national security. The decision of the Secretary or Deputy Secretary shall be conclusive and final.

B. Within the limits permitted by applicable laws, regulations, and instructions that are binding upon the Department, exceptions to the provisions of this chapter may be granted by the Director.

C. In accordance with the Inspector General Act of 1978; the Whistleblower Protection Act of 1989; and Presidential Policy Directive-19 (PPD-19), Protecting Whistleblowers with Access to Classified Information, no actions recommended in this chapter, regarding the continued eligibility for access to NSI, shall be used as reprisal for protected disclosures as defined in PPD-19. In instances where an employee alleges an officer or employee of the Department has taken, directed others to take, recommend, or approve any action affecting the employee's eligibility for access to classified information, an appeal is permitted to the Department Office of the Inspector General (OIG). The OIG will determine whether an action affecting clearance eligibility violated such protection.

The Director for Security, on behalf of the agency head, will implement corrective action, as appropriate, including reconsideration of the employee's eligibility for access to NSI, following the findings and recommendations of the OIG. The Director for Security will consult with the Director of OHRM regarding the restoration of the employee, as nearly as practicable and reasonable, to the position such employee would have held absent reprisal, consistent with the requirements of PPD-19.

The employee has the right to appeal the OIG decision to an Inspector General External Review Panel, consisting of a three-member Inspector General (IG) panel, chaired by the IG for the Intelligence Community (IC). It is the discretion of the chair of the IG for the IC to accept the appeal. The External Review Panel will not include a member of the OIG at Department.

If the appeal is accepted by the IG for the IC and the External Review Panel determines that the employee was the subject of an action affecting his or her eligibility for access to NSI, as reprisal for protected disclosures in violation of PPD-19, the panel may recommend 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. The Director for Security shall then reconsider the employee's continued eligibility for access to NSI consistent with the national security and Executive Order 12968, Access to Classified Information.

The Director for Security has 90 days to inform the panel and the Director for National Intelligence, on what action the Department has taken, following the findings and recommendations of External Review Panel.

The entire review process must provide for the protection of NSI and intelligence sources and methods.

14.12. REEMPLOYMENT OF TERMINATED EMPLOYEES

No person whose employment has been terminated by the Department under the provisions of 5 U.S.C. § 7532, E.O. 10450, as amended, E.O. 12968, E.O. 13467, or any other security or loyalty program, shall be reinstated, restored to duty, or reemployed in the Department unless the Secretary finds that such employment is clearly consistent with the interests of national security. No person whose employment has been terminated by any department or agency, other than the Department, under 5 U.S.C. § 7532, E.O. 10450, as amended, E.O. 12968, E.O. 13467, or any other security or loyalty program, shall be employed in the Department unless the Secretary finds that such employment is clearly consistent with the interests of national security and unless OPM determines that such person is eligible for such employment. The finding of the Secretary and the determination of OPM shall be made a part of the personnel security file of the person concerned.

Chapter 15. Special Access

15.1. Special Access Programs

Special access programs have been established to impose controls beyond those normally required for access to information classified as Confidential, Secret, or Top Secret. Under this definition, any classified program requiring additional controls could be considered a special access program. Such programs may require special clearances, special investigative requirements and/or special briefings. This chapter describes those special programs and procedures associated with granting access.

15.2. Special Access Program Policies

A. Requisite security investigations must be favorably completed before an individual can be granted access to information covered under special access programs. Department of Commerce (Department) employees who require information on obtaining authorization for access to any special access program not covered in this chapter or elsewhere in this Manual of Security Policies and Procedures should contact the Office of Security (OSY).

B. Supervisors or managers must notify their Servicing Security Office (SSO) immediately upon discovery of any information that indicates that an individual's current involvement in a special access program may not be in the national interest.

C. When access to one of the special programs is no longer needed, the supervisor or manager must initiate immediate action for administrative withdrawal. In most cases, a termination statement signed by the individual is required. Supervisors or program managers should contact their SSO for guidance.

D. Employees in special access programs who require a Top Secret security clearance must possess a favorably adjudicated Single Scope Background Investigation (SSBI), and/or a current SSBI–Periodic Reinvestigation (SSBI-PR). In addition, an SSBI-PR will be required every five years.

E. Special access programs usually require a prerequisite Departmental security clearance; however, a Departmental security clearance will not be issued exclusively for the purpose of granting special access.

F. Access to one of the special programs may be terminated for administrative reasons unrelated to an adverse security determination. An administrative termination of special access does not prejudice a person's eligibility for future access to a special program. On the other hand, revocation of special access program participation will be administered under the provisions of Chapter 14, Suspension, Revocation, and Denial of Access to Classified National Security Information.

15.3. Special Access Program Interagency Agreement

Special access programs may require an interagency memorandum of understanding (MOU) establishing the procedures and conditions under which an agency shall provide special access information to the Department. This agreement obligates the Department to maintain effective

security control of special access information. Special access programs cannot be established within the Department without prior approval from the Director for Security (Director) and/or the sponsoring agency.

15.4. SENSITIVE COMPARTMENTED INFORMATION (SCI)

Particular categories of classified intelligence information require special security access, special handling, and special storage facilities not covered by procedures for Confidential, Secret, and Top Secret information. Special markings are prescribed in directives, regulations, and instructions relating to SCI. Agencies within the Intelligence Community have responsibility for maintaining the security control of classified foreign intelligence materials furnished to governmental organizations that are not part of the Intelligence Community, such as the Department. These intelligence materials should not be confused with Foreign Government Information (FGI), which is described in Chapter 26, Foreign Government Information. See Chapter 12, Access to Classified National Security Information for procedures to request access to SCI.

15.5. CONDITIONS FOR SPECIAL ACCESS TO SCI

The Department's SCI program is sponsored by the Central Intelligence Agency (CIA) pursuant to a MOU between the Department and the member agencies of the Intelligence Community. The CIA maintains cognizance of the security aspects of Departmental approvals for access to, and receipt, handling, storage, and destruction of, foreign intelligence information. Under the MOU, the Department must comply with the directives and regulations that govern access to SCI such as the Intelligence Community Directive number (ICD 704), Personnel Security Standards and Procedures Governing Eligibility For Access To Sensitive Compartmented Information and other Controlled Access Program Information.

15.6. REQUEST FOR SPECIAL ACCESS TO SCI

A. OSY Counterespionage Division (CED) will submit requests for SCI access to the CIA. Once CED has been notified that SCI access has been approved, OSY or a designated agency official will conduct the SCI indoctrination.

B. An individual denied SCI access based on an investigation may appeal the decision within 45 days of notification of the denial. Procedures for appeal are shown in Intelligence Community Policy Guidance 704.3, Denial or Revocation of Access to Sensitive Compartmented Information, other Controlled Access Program Information, and Appeals Processes. The SSO should contact OSY for assistance.

C. An SCI Nondisclosure Agreement, Form 4414, will be signed by the employee after receiving an SCI indoctrination. When access is no longer required, an employee will receive a security debriefing and sign a debriefing acknowledgment. The security debriefing will also be required for separation, transfer, change in duties, suspension, or revocation of access. A copy of the signed Nondisclosure Agreement will be retained in the employee's personnel security file, and the original document will be forwarded to the CIA.

15.7. SCI Security Education

OSY shall administer a continuing security education program for all Departmental personnel authorized access to SCI. Under the program, employees with SCI access shall be reminded of their obligation to properly handle and safeguard SCI materials and of the potential consequences to the U.S. Government of any compromise or unauthorized use of such information. This reminder shall be given to the employee at least annually through an SCI refresher briefing or through another form of instruction.

15.8. Foreign Travel Requirements for SCI Access Holders

Departmental employees who have been granted access to SCI shall comply with special security requirements established to safeguard such information. The safeguarding requirements for SCI access shall be observed at all times, especially during travel. Each SCI-cleared employee in the Department who conducts official or unofficial travel outside the United States must contact OSY to arrange for a defensive security briefing prior to such travel. OSY shall determine the briefing requirement for each specific country visited.

15.9. Accreditation of Sensitive Compartmented Information Facilities

SCI material can only be maintained in facilities approved and accredited by the CIA for its receipt, storage, processing and handling. To request establishment and accreditation of a Sensitive Compartmented Information Facility (SCIF), forward a request through the Director, Office of Executive Support, to OSY. The request must include the SCI level of accreditation desired, complete address, point of contact, justification, and a description of any automated equipment that will be housed in the area. OSY will then arrange a physical security survey. OSY and a CIA Point of Contact will provide recommendations for any security upgrades in accordance with ICD 705, Sensitive Compartmented Information Facilities. After implementing the recommendations and concurrence by the CIA, a follow-up inspection will be conducted by the CIA prior to final accreditation. A final accreditation shall be provided in writing by the CIA to the head of an operating unit and a copy to the SSO. A file copy of the accreditation will be maintained in OSY CED.

15.10. North Atlantic Treaty Organization (NATO) Security Clearance

The NATO security clearance is governed by the United States Authority, NATO (USSAN). Access to NATO Classified National Security Information (NSI) requires an equivalent level U.S. security clearance and a special NATO briefing. The request package is the same as that for the equivalent U.S. security clearance except that the CD-79, Request for Security Clearance, is annotated as relating to access to NATO NSI. The request package is forwarded through the SSO directly to OSY CED, which will arrange for the appropriate NATO briefing. Before being granted access to NATO NSI, the employee must sign a NATO briefing acknowledgment form. A debriefing acknowledgment form is required when the access is terminated. Refer to Chapter 12 for the access requirements for NATO information.

15.11. Department of Energy (DOE) "Q" and "L" Security Clearances

The security clearances labeled "Q" and "L" are part of the DOE program for protection of information as required by the Atomic Energy Act of 1954 (10 CFR Part 95.31 and 42 U.S.C. § 2014 and §2162). A "Q" clearance is equivalent to a Top Secret clearance, while an "L" clearance is equivalent to a Secret clearance. These clearances may be granted only by the DOE based on an individual's need for access to the information and favorable adjudication of the appropriate clearance. The request packages should be sent directly through the SSO to OSY CED. See Chapter 12 for the access requirements for DOE Q and L information.

15.12. Cryptographic Clearance

A. Certain U.S. classified communications security (COMSEC) information/material requires special access restrictions. OSY administers the COMSEC program. Bureaus and operating units requiring COMSEC access should contact the SSO to coordinate needs with OSY headquarters. COMSEC information is specified as either of the following:

1. Top Secret and Secret, CRYPTO designated, key, and authenticators.
2. Classified cryptographic media that embody, describe, or implement a classified cryptographic logic, such as full maintenance manuals, cryptographic descriptions, drawings of cryptographic logics, specifications describing a cryptographic logic, and cryptographic computer software.

B. An individual may be granted access to COMSEC information based on fulfillment of all of the following requirements:

1. Maintains U.S. citizenship.
2. Is employed by the U.S. Government, or represents the U.S. Government, or serves as a Government contractor, or is employed by a contractor.
3. Requires access to perform official duties for, or on behalf of, the Department.
4. Possesses a Department security clearance appropriate to the classification level of the COMSEC information to be accessed.
5. Receives a security briefing appropriate to the COMSEC information to be accessed.
6. Acknowledges the granting of access by signing a Cryptographic Access Certificate.
7. When required, consents to the administration of a periodic counterintelligence (CI)-scope polygraph examination. The polygraph examination will encompass questions concerning espionage, sabotage, and unauthorized giving or selling of NSI to, or unauthorized contacts with, representatives of foreign governments or agencies. OSY will arrange the polygraph examination when required.

C. The requirements listed above apply to all individuals whose primary assignment allows continuous, long-term access to COMSEC information in large quantities or with highly

sensitive applications. Accordingly, these requirements apply specifically to the following personnel.

1. COMSEC custodians or alternates.
2. Producers or developers of cryptographic key or logic.
3. Personnel assigned to the major supply points where cryptographic keying materials are generated or stored.
4. Couriers in the Defense Courier Service.
5. Personnel assigned to secure telecommunications facilities located in fixed ground facilities or onboard ships.
6. Specialists who prepare, authenticate, or decode valid or exercise nuclear control orders.
7. Anyone else who has access to classified cryptographic media.

15.13. CERTIFICATION OF SPECIAL ACCESS

A. Transmitting Security Access Information.

Visits to Other Government Agencies Requiring SCI Clearance. The SSO shall provide the following information to OSY CED at least five working days in advance of the proposed visit.

1. Requestor's name and phone number.
2. Visitor's name, date and place of birth, and Social Security number (SSN).
3. Special access required.
4. Name and location of the agency to be visited.
5. Date range of the proposed visit.
6. Name and telephone number of the point of contact for the project/program causing the visit.
7. Purpose of visit: (unclassified description).

B. Personnel Transfers.

1. **Transfers to Another Government Agency**. The SSO is responsible for notifying OSY CED of all employee transfers. However, OSY CED will handle agency requests for special access program information processing bases, and security file review. All such inquires received by the SSO shall be directed to OSY CED.
2. **Transfers Within a Department Operating Unit But Between SSO Jurisdictions.** The relinquishing SSO shall forward, in a timely manner, a copy of the employee's Security Index record to the gaining SSO. The gaining SSO will be responsible for incorporating the security record information into their Security Index and advising

OSY CED in writing of the change in jurisdiction and any change in position title, position sensitivity, and/or level of security clearance needed. The receiving SSO must process upgrades or downgrades of security clearance, and any adjustments to position designation.

3. **Transfers to Different Department Operating Units Within the Same SSO's Jurisdiction.** The SSO is responsible for informing OSY CED, in writing, of the employee's new operating unit, position title, change in position designation, if any, and new security clearance needs, if any.

4. **Special Access Does Not Automatically Transfer With the Individual**. Security clearances do not transfer with an individual, and therefore, neither does special accesses. Any permanent change in operating unit, or even a significant change of duties within the same operating unit, requires that the access be requested again and re-justified using Form CD-79 and a SCI Request Memorandum with justification of access required in the new position.

SECTION III. CLASSIFIED NATIONAL SECURITY INFORMATION

Chapter 16. Classified National Security Information Policies

16.1. PURPOSE

This Department of Commerce (Department) Manual of Security Policies and Procedures (Manual) prescribes the policies, procedures, and standards that govern the safeguarding of Classified National Security Information (NSI). Section III of the Manual implements Executive Order (E.O.) 13526, Classified National Security Information, and establishes a system for classifying, declassifying, and downgrading NSI. Section III provides guidance for the enforcement and management of security responsibilities and the procedures for reporting, reviewing, and recording security infractions and violations. The provisions of this section set forth the minimum security standards and safeguards to ensure protection of NSI in the Department.

16.2. APPLICATION

A. In a Presidential Order signed October 13, 1995, the President of the United States conferred classification authority on the Secretary of Commerce to originally classify information at the Secret classification level. Departmental Organization Order (DOO) 20-6 designates the Director for Security (Director) as the "senior agency official" to direct and administer the Department NSI program implementing E.O. 13526, under which information is classified, safeguarded, and declassified.

B. The NSI policies, procedures, and standards prescribed in this chapter apply to employees and applicants for employment with the Department, as well as contractors, guest researchers, committee members, students and trainees, and other persons designated by the Secretary of Commerce for access to NSI. In addition, managers, supervisors, and employees are responsible for familiarization and compliance with all personnel security regulations and procedures at their respective installations.

C. Questions concerning policies pertaining to NSI should be referred to the Office of Security (OSY) through the Servicing Security Office (SSO). Policy interpretations should be addressed to OSY. The Director shall provide the Department's interpretation of policies and procedures concerning the protection of NSI, and, as necessary, provide written guidance to operating units and other Departmental offices.

16.3. NSI POLICIES

Policies for the Department's NSI program are outlined below.

A. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life. Our national interest requires that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Accordingly, classifying authorities, program managers, supervisors, and

employees shall follow the provisions of E.O. 13526, or subsequent orders, to protect NSI.

B. Our nation's democratic principles also require that the American people be informed of the activities of their Government; therefore, information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security. If there is significant doubt about the need to classify information, the information shall not be classified. If the classifying authority has a significant doubt about the appropriate level of classification, he or she will classify the information at the lower level. In addition, NSI shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

C. The authority to classify original information at the Secret or Confidential level may be exercised only by the Secretary of Commerce and officials to whom Original Classification Authority (OCA) has been delegated. No Departmental official is authorized to classify original information at the Top Secret level. Officials authorized to classify information at the Secret level are also authorized to classify information at the Confidential level.

D. The delegation of OCA will be limited to the minimum number of individuals absolutely required for the efficient administration and protection of programs in the Department. Classification authority delegated by the Secretary cannot be re-delegated but may be exercised by persons designated in writing to act in the absence of the designated classifying authority, provided they have the appropriate level of security clearance and have received OCA training from OSY.

E. Derivative classification includes the classification of information based on a classification guide or classified source document. The duplication or reproduction of existing NSI is not derivative classification. With the appropriate security clearance, Department employees involved in the production or generation of information based on previously NSI are authorized to derivatively classify information.

F. E.O. 13526, encourages authorized holders of NSI to challenge classification decisions as a means of promoting proper and thoughtful classification actions. Authorized holders wishing to challenge the classification status of information shall present such challenges to a classification authority that has jurisdiction over the information. A formal challenge under this provision shall be in writing and coordinated with OSY.

G. Information that continues to meet the classification requirements of E.O. 13526, or subsequent orders, requires continued protection; however, Department information shall be declassified as soon as it no longer meets the standards for classification under this E.O. When NSI is transferred from another agency or operating unit in conjunction with a transfer of functions, and not merely for storage purposes, the receiving operating unit shall be deemed the originating office for purposes of downgrading and declassification.

H. Each operating unit that holds NSI shall establish and implement procedures for systematic declassification. This program shall apply to historically valuable records exempted from automatic declassification under E.O. 13526. Operating units shall

prioritize the systematic review of records based on the degree of researcher interest and the likelihood of declassification upon review. Operating units or offices shall maintain a current listing of officials delegated declassification authority by name, position, or other identifier. If possible, this list shall be unclassified.

I. Unless properly exempted from automatic declassification, all NSI contained in records that are more than 25 years old and that have been determined to have permanent historical value under Title 44 of the U.S. Code shall be automatically declassified whether or not the records have been reviewed.

J. NSI under Department jurisdiction must be reviewed for declassification upon receipt of a request by a U.S. citizen or permanent resident alien, a federal agency, or a state or a local government. A request for mandatory review of NSI shall be submitted in writing and describe the information with sufficient specificity to locate it with a reasonable amount of effort.

K. The head of each operating unit must establish procedures for the control and accountability of Top Secret, Secret, and Confidential information by use of written records or an electronic database. Each operating unit shall designate an office/unit classified control point. The operating unit may request exceptions. Procedures shall ensure that the movement of NSI can be traced, its dissemination is limited, the retrieval of information can be executed promptly, the loss of information can be detected, and excessive holdings and reproduction are limited. Offices maintaining NSI must conduct an annual inventory and review their classified holdings. Each document must be visually inspected upon initial receipt and during the annual inventory to ensure that the document is complete or accounted for by written evidence of proper disposition. This inventory shall include a review to determine possible downgrade, declassification, or destruction of classified holdings to reduce the amount necessary for operational and program purposes. The results of this inventory shall be forwarded to the Security Contact or SSO.

L. Federal employees are not automatically cleared for access to NSI. The number of personnel cleared and granted access to NSI in the Department should be maintained at the minimum number consistent with operational requirements and needs. When a person no longer needs access to a particular security classification level, the security clearance should be adjusted, or downgraded, to the classification level required for the performance of the person's official duties and obligations. The administrative downgrade or withdrawal of an individual's security clearance does not prejudice the person's eligibility for a future security clearance.

M. No employee has a right to gain access to NSI solely by virtue of title, position, or level of security clearance. An employee is eligible for access to NSI provided the employee has been determined to be trustworthy by the appropriate investigation, has executed a Standard Form-312, Classified Information Nondisclosure Agreement, and requires access to accomplish lawful and authorized Government purposes.

N. NSI (in any form), including extra copies, is not personal property and may not be removed from the Government's control by any departing official. The head of each

operating unit and the SSO shall ensure that all separating personnel account for all NSI in their possession and transfer all classified material to an authorized custodian.

O. Heads of operating units must ensure that only authorized persons obtain access to NSI; however, the final responsibility for determining whether an individual obtains access to NSI rests with the individual who has possession, knowledge, or control of the information and not with the prospective recipient. NSI must be protected at all times by the holder of the information. Before NSI is disclosed, the holder must verify the recipient's identification and security clearance through his or her operating unit's SSO or Security Contact, determine the recipient's need to know, and advise the recipient of the classification level of the information.

P. NSI may be transmitted by authorized means both inside and outside of the Department; however, NSI may be hand-carried aboard commercial passenger aircraft only when there is neither time nor means available to properly transmit the information by other authorized means and authorization is granted by the Director for Security (Director). The Director may grant permission to courier classified material overseas on a case-by-case basis. Requests for permission to courier NSI aboard a commercial passenger aircraft shall be submitted in writing to OSY CED through the SSO prior to departure.

Q. SSOs may authorize an employee to hand-carry NSI up to the Top Secret level within the United States and its territories. To be an authorized courier, the employee must hold an appropriate security clearance and possess a valid Courier Authorization Card (CD-75) or Courier Authorization letter assigned by the SSO. All couriers must review the Guidelines and Authorization for Couriers and sign the Acknowledgement of Guidelines for Couriers of National Security Information for return to the SSO.

R. NSI must be stored under conditions that will provide adequate protection against access by unauthorized persons. Whenever NSI is not under the personal control and observation of a cleared person, it must be guarded by personnel with the appropriate security clearance or stored in a locked General Services Administration-approved security container. An office that receives NSI (in any form) and has no authorized storage equipment available must either return the NSI to the sender, arrange with another office to properly store the information, or destroy it by an approved method. Under no circumstances shall NSI be left unattended, in an unauthorized storage container, or in the custody of a person who does not have the proper security clearance and an established need to know.

S. The head of an operating unit or the SSO may determine that more stringent requirements are needed based on the volume, nature, and sensitivity of the information to be protected in relation to other factors such as types of containers, presence of guards, vault-type space, or intrusion alarms. Bulky Secret and Confidential information may be stored in vaults or other closed areas; however, no area shall be used for classified open storage without prior accreditation and written approval from OSY.

T. The head of each operating unit responsible for protecting NSI will develop and implement procedures to protect incoming mail, bulk shipments, and items delivered by

messenger that contain classified material. Procedures shall be established at receipt points to limit access to NSI to cleared personnel only.

U. Classified documents shall be destroyed in a manner sufficient to preclude recognition or reconstruction of the NSI. The heads of operating units shall ensure that procedures are established for the proper destruction of NSI in their operating unit. Such procedures must ensure that adequate destruction records are maintained, authorized destruction methods are used, information is protected during transport, and the destruction is properly witnessed. Classified documents may be destroyed only by authorized methods.

V. NSI shall not be discussed over, or otherwise transmitted or processed by, any form of telecommunications unless approved measures are taken to protect the information. Basic policies dealing with the security of federal telecommunications are developed and issued under the purview of the National Security Council. The National Security Agency (NSA) issues implementing instructions. This Manual implements the NSA security requirements governing communications security equipment and operations. In addition, operating systems processing NSI shall be reviewed every three years for certification and accreditation or when major changes are made to the system.

W. All security incidents, violations, or compromises must be reported through the SSO to OSY headquarters. Any person who has knowledge or suspects the loss or possible compromise of NSI (in any media), or any person who discovers NSI out of proper control, including NSI discovered improperly safeguarded and left unattended and unsecured, shall immediately take custody of such information, safeguard it in an appropriate manner, and report the loss or possible compromise to OSY headquarters through the SSO.

X. Each security violation or infraction shall be noted on the employee's performance evaluation, may result in a review of security clearance retention, and shall be referred to the operating unit to determine whether disciplinary action is warranted. Based on a security violation reported and validated, OSY may suspend access to NSI.

Y. OSY Counterespionage Division (CED) personnel, SSOs, and OSY/CED personnel are responsible for conducting random after-hours inspections to ensure that NSI is properly protected and secured. Persons participating in these official inspections are authorized to enter any office under the actual control and/or possession of the Department and/or any subordinate operating unit at any time. Designated security personnel are authorized to conduct such inspections in the performance of their official duties. This inspection may consist of a search of desktops, desk drawers, cabinets, or other miscellaneous office furniture and equipment within the confines of a Government-owned or leased building used by Department or operating unit personnel. The purpose of the inspection is to ensure that classified and critically sensitive information is being protected properly. Inspections involving Department office space occupied by employees of, or under the control of, another agency shall be coordinated with the other agency.

16.4. STATUTORY REQUIREMENTS

A. Nothing in these regulations shall be construed as authorizing the dissemination, handling, or transmission of information contrary to the provisions of any statute. In any conflict, specific statutory provisions shall prevail.

B. Invention Secrecy Act.

1. **Classified Patent Documents:** Patent applications and certain related documents are subject to the Invention Secrecy Act of 1951, as amended (35 U.S.C. §§ 181-188). which concerns the secrecy of certain inventions and related matters. These documents may contain information identified as NSI. When such documents contain NSI, they must be safeguarded in accordance with the provisions of this section of E.O. 13526, or subsequent orders.
2. **Applications Pending Review:** Patent applications that have not yet been reviewed for security classification should be safeguarded as Confidential NSI until the appropriate authority makes a classification determination.
3. **Unclassified Applications:** Unclassified patent applications on which a Type 1 Secrecy Order has been imposed do not require the safeguards afforded to NSI. These applications and related documents are subject to the export control laws and must be provided adequate protection to prevent access by unauthorized persons (50 U.S.C. § 2401 et seq.). The level of protection is normally less stringent than that required for NSI.

16.5. PROCEDURAL EXEMPTIONS

A. A request for an exception to the procedural provisions of this section must be made in writing to OSY and must set forth all salient facts, justifications, and a proposed alternate procedure. Some requests for waivers from the provisions of E.O. 13526, or implementing directives cannot be granted at the Departmental level. However, the Director will consider such requests and, if approved, will forward the request to the Information Security Oversight Office (ISOO) for a final decision.

B. The Director of the ISOO has determined that restrictions contained in E.O. 13526, do not apply to the use of the term "Confidential" in relation to data collected by the Bureau of the Census (Census). Title 13, U.S.C., enables Census to use the term "Confidential" as a guarantee to citizens of the United States that whatever personal and private information it collects will be protected from disclosure. Identifying data as "CENSUS Confidential" does not violate the provisions of E.O.13526, when the term refers to Census information and not to NSI.

16.6. REPORTING REQUIREMENTS

A. OCA. OSY shall maintain a current list of individuals in the Department, by position, who have been delegated OCA. The head of an operating unit shall notify OSY when a change occurs regarding delegations of authority within his or her operating unit.

B. **OCA Training.** All OCAs must receive training in proper classification (including the avoidance of over-classification) and declassification at least once a calendar year. Such training must include instruction on the proper safeguarding of NSI and on the sanctions that may be brought against an individual who fails to classify information properly or protect NSI from unauthorized disclosure. OCAs who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official designated under section 5.4(d) of E.O. 13526 until such training has taken place. OSY CED is responsible for providing the training, keeping track of training received and, reporting the information to ISOO yearly.

C. **Classification Actions.** OCAs and persons who apply derivative classification markings shall maintain records in the Security Manager database concerning original and derivative classification actions. The information provided in Security Manager will be matched with the corresponding information provided in the SF-311, Agency Security Classification Management Program Data. The information provided shall be an inspection item during OSY's yearly document inspection program. SSOs or Security Contacts shall review records and reports to ensure the information submitted by an OCA is complete and accurate.

D. **Inventory of Top Secret and Secret Documents.** OCAs will ensure that an inventory of Top Secret and Secret documents is maintained in either written or electronic form in their respective organizations. The bureau or operating unit shall inventory Top Secret and Secret documents and material at least annually, or more frequently when necessary. During the inventory, each document or item shall be physically reviewed and examined for completeness and accuracy or accounted for by examination of written evidence of proper disposition.

E. **Cost Estimates of Classification-Related Actions.** The heads of operating units will ensure that cost estimates associated with classification-related activities are reported through the SSO to OSY each October for the previous fiscal year. These classification-related activities include personnel security, classification management, electronic security, and other related activities. In addition to costs associated with classification activities, this report will include information concerning costs associated with declassification activities. These costs will be collected by OSY and transmitted directly to the ISOO. The Secretary of Defense, acting as the executive agent for the National Industrial Security Program under E.O. 12829, as amended, will collect the cost estimates for the classification-related activities of Departmental contractors, licensees, and federal advisory committee members, and report those costs to ISOO. ISOO is ultimately responsible for providing a final annual report to the President on these costs. All Secret documents printed from the Secret Internet Protocol Router Network shall be accounted for in Security Manager.

F. **Missing or Compromised NSI.** An employee who discovers that a classified document is either missing or compromised, or believes that a classified document is missing or

compromised, must verbally report the discovery to the appropriate SSO immediately following the discovery. In the case of a known or suspected compromise of NSI or special access program information, the SSO must report this information immediately and directly to OSY headquarters.

G. Contact with Foreign Nationals.

1. Employees must report contacts with foreign nationals (from any country) that do any of the following:
   a. Seek unauthorized access to sensitive or NSI
   b. Request unclassified or other publicly available information, particularly when there is an offer of exchange or payment of some kind, or if the request involves undue flattery or attention for the service performed.
   c. Display efforts to become friendly, no matter how innocuous.
   d. Offer help or assistance in performing duties or accomplishing tasks.
   e. Request the help or assistance of a specific employee outside of routine channels.
2. Employees must report information about this contact immediately through their SSO to OSY headquarters. The report shall include all of the following information:
   a. The name, office, and telephone number of the individual making the report and the date the report is submitted.
   b. The date and type of contact (e.g., business, social).
   c. The foreign national's name and address (business and residential), citizenship, or country.
   d. A description of the individual, including the sex, approximate height and weight, color of hair, color of eyes, and other distinguishing features.
   e. Whether the contact being reported was the first such contact with the individual, or, if there had been others, and the approximate date(s).
   f. A detailed narrative of the incident.

H. Other Security Reports. Each SSO or the designated Security Contacts shall submit the reports listed below to OSY headquarters in a timely manner.

1. **Classification Actions.** SSOs and Security Contacts shall submit the SF-311 to OSY headquarters by October 30 each year. This report covers original and derivative classification actions by an OCA for the previous reporting period.
2. **Top Secret and Secret Inventory Review.** Bureaus and operating units maintaining an inventory of Top Secret and Secret documents on an electronic database or in written format will submit certification of their inventory review to OSY headquarters by October 30 each year. The report shall reflect the inventory of Top Secret and Secret documents as of October 1.

Chapter 17. Security Classification

17.1. Classification Principles

The national interest requires that certain information be maintained in confidence through a system of classification to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life. However, our nation's democratic principles also require that the American people be informed of the activities of their Government; therefore, information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security. Accordingly, security classification shall be applied only to protect Classified National Security Information (NSI). With the exception of the Atomic Energy Act of 1954, as amended, and the National Security Act of 1947, as amended, Executive Order (E.O.) 13526, Classified National Security Information, provides the only basis for classifying NSI.

17.2. Original Classification Standards

A. Information may be originally classified under the terms of E.O. 13526, only if all of the following conditions are met.

1. An Original Classification Authority (OCA) classifies the information.
2. The information is owned by, produced by or for, or is under the control of the U.S. Government.
3. The information falls within one or more of the categories of information listed in Paragraph 17.5 below.
4. The OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage at the level of classification.

B. At the time of the classification decision, there is no requirement for the OCA to prepare a written description of such damage; however, the OCA must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand.

C. NSI shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

17.3. Classification Levels

A. NSI that requires protection against unauthorized disclosure shall be classified by an authorized OCA at one of the following three levels:

1. **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.

2. **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.

3. **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.

B. Except as provided by statute, no additional terms such as "Sensitive," "Agency," "Business," or "Administratively" shall be used in conjunction with any of the three classification levels defined above.

17.4. CLASSIFICATION AUTHORITY

A. E.O. 13526 states that the President will name agency heads and selected officials authorized to classify information in the *Federal Register*. The Secretary of Commerce (Secretary) is named by position in the *Federal Register* as having the ability to originally classify at the Secret or Confidential level. It is important to note that no Department of Commerce (Department) official is authorized to originally classify information at the Top Secret level.

B. The authority to classify original information in the Department may be delegated only to those positions that have a demonstrable and continuing need to exercise such authority. Incumbents occupying these positions must have a security clearance at the appropriate level. Classifying authority delegated by the Secretary cannot be reassigned but may be exercised by persons designated in writing to act in the absence of the designated classifying authority, provided they have the appropriate level of security clearance. The delegation of OCA will be limited to the minimum number of individuals absolutely required for efficient administration and protection of Departmental programs and receive the required training by the Office of Security (OSY).

C. Requests for delegation of authority to perform original classification actions shall be made to the Secretary through the Director for Security (Director). The request shall identify the proposed recipient by position, operating unit, and the level of classification authority requested. The request must also include adequate justification for the OCA delegation.

D. Prior to assigning a classification, an OCA shall refer to the Department National Security Classification Guide (see Paragraph 17.13) to determine whether the information considered for classification can be addressed in the classification guide. OCAs are encouraged to consult with their Security Contacts or their Servicing Security Office (SSO) for assistance when classifying information. OCAs shall keep records of all original classification decisions in the OSY Security Manager database and shall provide this information upon request to their SSO. This record is required to comply with internal review and evaluation requirements of E.O. 13526, as well as annual reporting requirements of classification decisions.

E. All original and derivative classification and declassification decisions must be documented in Security Manager and shall provide this information upon request to their SSO. To compile the necessary data, each OCA shall report all original and derivative classification and declassification decisions by maintaining accurate records of all decisions made. Effective recordkeeping is essential in compiling data for this annual requirement. All units having original or derivative classification authority must submit yearly statistics on the number of original and/or derivative classification actions, including "zero" if there was no activity. Input shall be submitted from each operating unit or SSO to OSY in Washington, DC. The SSO must retain the completed SF 311 with data provided by each OCA and unit head regarding original and derivative classification, and/or declassification decisions made during each fiscal year. All decisions may be challenged; therefore, file records must be maintained.

F. Each OCA shall ensure his or her operating unit records systems are designed and maintained to optimize the safeguarding of NSI and to facilitate the declassification of records under the provisions of E.O. 13526, when such information no longer meets the standards for continued classification.

G. On an annual basis, the Director shall review the continuing need for an OCA in each operating unit. The Director may recommend withdrawing classifying authority when no demonstrated or continuing need exists for the official to exercise this authority, upon failure of the official to provide adequate justification for continuing use of the authority, or if an official is in violation of one or more of the E.O. 13526 provisions. If a demonstrated or continuing need for an OCA should arise subsequent to a revocation, a new request for delegation shall be submitted.

H. OSY shall provide or ensure OCA training is conducted as directed by E.O. 13526 .

17.5. CLASSIFICATION CATEGORIES

Information may be classified when it concerns one or more of the categories listed below, and when the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Information may only be considered for classification if it concerns the categories listed below.

A. Military plans, weapons systems, or operations.

B. Foreign government information.

C. Intelligence activities (including cover actions), 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. U.S. 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. The development, production, or use of weapons of mass destruction.

17.6. DURATION OF CLASSIFICATION UNDER E.O. 13526

A. OCAs shall follow the sequence listed below when determining the duration of classification for information originally classified under E.O. 13526, Classified National Security Information.

1. At the time of original classification, the OCA shall attempt to establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. The date or event shall not exceed the time frame noted below.

2. If an OCA cannot determine a specific date or 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 shall be marked for declassification for up to 25 years from the date of the original decision. All information classified according to guidance contained in E.O. 13526, shall be subject to automatic declassification provisions if it contains records of permanent historical value.

3. An OCA may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under E.O. 13526, are followed. An OCA may extend the duration of classification for information contained in non-permanent records beyond 25 years in accordance with the standards and procedures for classifying information under E.O. 13526, except for information that identifies a confidential human source or a human intelligence source. However, the OCA shall identify a specific date or event for declassification of the information when extending the classification beyond 25 years.

4. When extending the duration of classification, the OCA must do all of the following:
   a. Have jurisdiction over the information.
   b. Ensure that the information continues to meet the standards for classification under E.O. 13526.
   c. Make reasonable attempts to notify all known holders of the information.

B. Extensions of classification are not automatic. If an OCA with jurisdiction over the information does not extend the classification of information that has an assigned date or event for declassification, the information is automatically declassified upon the occurrence of the date or event.

C. When attempting to determine a date or event for declassification, it is not permissible to use the term "Originating Agency Determination Required" or "OADR." This term was acceptable under a previous Order but is no longer permitted. Records marked as such are not appropriately marked. Historical records marked as "OADR" shall be declassified.

1. A declassification authority with jurisdiction over the information may declassify the information and release it unless withholding it is otherwise authorized and warranted under applicable law.
2. An authorized OCA with jurisdiction over the information may specify a date or event for declassification.
3. Unless declassified earlier, such information contained in records determined by the Archivist of the United States to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to automatic declassification procedures of E.O. 13526.

Note: It is recommended that each year during the annual classified material inventory, all classified documents be reviewed and evaluated for further retention, possible declassification, or destruction.

17.7. TENTATIVE CLASSIFICATION

When an employee, contractor, licensee, certificate holder, or grantee of the Department that does not have the authority to make original classification decisions develops information requiring classification, the individual shall safeguard the information in the manner prescribed according to its intended classification. The developer shall forward the tentatively NSI to an appropriate OCA for a classification decision. OCAs will have 30 days from the date of the classification request to make a classification determination. If it is not clear which OCA has classification responsibility for this information, the holder of the information shall forward the information, with appropriate recommendations, to the Director to determine which OCA has primary subject matter interest. OSY maintains a list of senior executives who have been granted OCA. If it cannot be determined which OCA has primary subject matter interest, the Director will make a classification decision on behalf of the Department or forward the information to the Director of the Information Security Oversight Office (ISOO) for a determination.

17.8. LIMITATIONS ON CLASSIFYING INFORMATION

A. Information shall not be classified for any of the following purposes:

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.

B. Basic scientific research information not clearly related to the national security shall not be classified.

C. Information may be reclassified after declassification and released to the public under proper authority only in accordance with all of the following conditions:

1. The reclassification action is taken under the personal authority of the Secretary or Deputy Secretary of Commerce, who determines in writing that the reclassification of the information or documents is necessary in the interest of the national security.
2. The information or documents may be reasonably recovered.
3. The reclassification action is reported promptly to the Director of ISOO.

D. Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after the Department has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory declassification review provisions of E.O. 13526, only if such classification meets the requirements of the E.O. and is accomplished on a document-by-document basis under the direction of the Director.

E. Compilations or aggregation of preexisting items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that satisfied both of the following conditions:

1. Meets the standards for classification under E.O. 13526.
2. Is not otherwise revealed in the individual items of information.

F. There are specific actions an agency must take if it wants to reclassify information that has previously been disclosed to the public. For specific instructions, contact OSY.

17.9. CLASSIFICATION CHALLENGES

A. E.O. 13526, authorized holders of information, who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under Sec. 1.8 of E.O. 13626. An authorized holder is any individual, including an individual external to the agency, who has been granted access to specific NSI in accordance with Section 4.2(a) of E.O.13526. Authorized holders shall present such challenges to an OCA who has jurisdiction over the information. A formal challenge under this provision shall be in writing and coordinated with OSY. The challenger shall include a statement of why he or she believes the information should or should not be classified at a different level.

B. Classification challenges shall follow the procedures outlined below.

1. OSY shall maintain a system for processing, tracking, and recording formal classification challenges made by authorized holders. Records of challenges shall be subject to oversight by the Interagency Security Classification Appeals Panel. Classification challenges shall be considered separately from Freedom of Information Act or other access requests.
2. OSY shall ensure that each challenge is reviewed by an OCA with jurisdiction over the challenged information. If the challenger is not satisfied with the decision, the

challenger may request a review by an impartial official or panel of the originating agency.

3. The OCA reviewing a classification challenge shall provide a written response to a challenger within 60 days. If the OCA is unable to complete his or her review of the classification challenge within 60 days, the OCA must notify OSY and provide a date by which he or she will respond. OSY will inform the challenger and state that if no response from the OCA 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 Interagency Security Classification Appeals Panel if the Director has not responded to an internal appeal within 90 days of the receipt of the appeal.

C. Denied challenges shall include all of the following, at a minimum:

1. A concise reason for denial of the challenge, unless such reason would reveal additional NSI.
2. The names or titles of the officials reviewing the challenge.
3. The challenger's rights to appeal, including procedures for forwarding the appeal to the Interagency Security Classification Appeals Panel. The Department is not required to process a challenge on information that has been the subject of a challenge within the past two years or the subject of pending litigation. OSY shall inform the challenger of his or her appeal rights.

D. Challengers and OCAs should attempt to keep all challenges, appeals, and responses unclassified. However, NSI is contained in a challenge, a Departmental response, or an appeal shall be handled and protected in accordance with E.O. 13526 and its implementing directives. Information being challenged for classification shall remain classified unless and until a final decision is made to declassify it.

E. The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such informal inquiries should be used as a means of minimizing the number of formal challenges.

17.10. DERIVATIVE CLASSIFICATION

A. Unlike original classification, derivative classification is incorporating, paraphrasing, re-stating, or generating in a 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 includes the classification of information based on classification guidance. The duplication or reproduction of existing NSI is not derivative classification. With the appropriate security clearance, Departmental employees involved in the production or generation of information based on previously NSI are authorized to derivatively classify information.

B. The overall classification markings and portion markings of the source document should supply adequate classification guidance to the derivative classifier. If portion markings or classification guidance are not found in the source document and no reference is made to an applicable classification guide, guidance should be obtained from the originator of the source document. If such markings or guidance are not available, the derivative classifier shall classify and portion mark the extracted information using the overall classification of the source document.

C. Personnel applying derivative classification to classified material shall follow the guidance noted below.

1. Persons who only reproduce, extract, or summarize NSI or who only apply classification markings derived from source material or as directed by a classification guide, need not possess OCA. Persons who apply derivative classification markings shall do all of the following:
   a. Observe and respect original classification decisions.
   b. Carry forward the pertinent classification markings to newly created documents.
   c. Apply the date or event for declassification that corresponds to the longest period of classification when the information is based on multiple sources.
   d. Attach a listing of classified source(s) to the official file or record copy.
   e. Maintain a copy of the source document, or information identifying the source document, with the record or file copy of the newly created document.
2. If the derivative classifier disagrees with the classification of a source document, the classifier may challenge the original classification decision through OSY.

17.11. POLICY ON TRANSFER OF SCIENTIFIC, TECHNICAL, AND ENGINEERING INFORMATION

National Security Decision Directive 189 is the national policy for controlling the flow of science, technology, and engineering information produced in federally funded fundamental research at colleges, universities, and laboratories. This directive requires federal agencies to do both of the following:

A. Determine whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, control the research results through standard classification procedures.

B. Periodically review all research grants, contracts, or cooperative agreements for potential classification.

17.12. DEVELOPMENT AND USE OF THE DEPARTMENT OF COMMERCE CLASSIFICATION GUIDE

A. A classification guide is written guidance issued for a particular program, project, or class of documents to ensure proper and uniform classification of information. The Department's sample National Security Classification Guide (see Paragraph 17.13) has been developed to establish uniform classification guides for frequently recurring items of classified NSI throughout the Department. The Guide consists of a series of predetermined classification decisions that individuals who are authorized to exercise

OCA may reference when making classifying decisions. The use of an item in the Guide to classify a document is considered a derivative classification decision.

B. OCA is not required for individuals using the guide. Employees who generate information that requires classification are authorized to derivatively classify that information by citing the applicable item in the guide and applying the classification level. Employees also will indicate the date or event for declassification that the Guide prescribes. Officials occupying OCA-delegated positions should invoke original classification only when no appropriate item can be identified in the Guide.

C. When an original classification decision is applied to a category of information not covered, inadequately covered, or improperly covered by the Guide, the classifier or responsible component should inform OSY. When it becomes apparent that classification is applied to information not covered or inadequately covered in the Guide, then OSY will take action to update the Guide. The Guide is the standard reference for national security classification actions in Department and, therefore, is continuously subject to review and update.

D. An OCA may elect to develop a supplemental classification guide that is specific to his or her program area. Guides are needed to identify information that truly warrants protection in the interests of national security and to expedite classification decisions. A guide should do all of the following:

1. Identify the subject matter of the classification guide.
2. Identify the OCA by name or identifier and position.
3. Identify an agency point-of-contact for questions regarding the classification guide.
4. Provide the date of issuance or last review.
5. State precisely the elements of information to be protected.
6. State which classification level applies to each element of information and, when useful, specify the elements of information that are unclassified.
7. State, when applicable, special handling requirements.
8. Prescribe declassification instructions or the exemption category from automatic declassification for each element of information. When reviewing or updating a guide, the duration of classification prescribed for each element of information shall be calculated from the date of the information's origin. In addition, when citing the exemption category listed in Paragraph 18.4, Automatic Declassification, the Guide shall also specify the applicable statute, treaty, or international agreement.
9. State a concise reason for classification that, at a minimum, cites the applicable classification category or categories in Paragraph 17.5.

E. Classification guides should be prepared in all areas where there exists a demonstrated need for a guide. Each classification guide shall be approved in writing by the

individual who has program or supervisory responsibility for the information and has been delegated OCA at the highest level prescribed in the guide. The classification guide shall be coordinated with OSY.

F. Originators of classification guides are encouraged to consult the users of guides for input when reviewing or updating guides. In addition, users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide. Classification guides shall be reviewed and updated as circumstances require but, as a minimum, at least once every five years.

17.13. SAMPLE DEPARTMENT OF COMMERCE CLASSIFICATION GUIDE

A. General.

1. **Purpose**. This sample classification guide is issued for the purpose of identifying specific topics of information associated with the bureaus within the Department that meet the standards and criteria for classification and protection in accordance with E.O. 13526, Classified National Security Information.

2. **Authority.** This guide is approved by the Director, OSY, also serving as a designated Secret OCA. It is issued in accordance with E.O. 13526 and ISOO Directive No. 1 (32 CFR, Part 2001/2004), "Classified NSI," Final Rule.

3. **Scope and Applicability**. This document provides security classification guidance for information associated with Departmental essential missions and activities. This may include international trade policy and development, and radio frequency and spectrum information and satellite services. This guide shall be cited as the basis for classification of information and materials for the Department. Changes in guidance required for operational necessity will be made immediately upon notification and concurrence of the approving authority and will be disseminated to original recipients of this guide. The provisions of this guide are applicable to all organizational entities and contractors associated with the Department.

4. **Office of Primary Responsibility**. The Office of Primary Responsibility (OPR) for this guide is:
   U.S. Department of Commerce
   Office of Security
   14th & Constitution Ave., NW
   Washington, DC 20230
   Telephone: (202) 482-8115
   Fax: (202) 501-2488

B. Policy.

1. **Reason for Classification**. Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause

identifiable or describable damage to the national security in accordance with section 1.2 of E.O. 13526, and it pertains to one or more of the following:

- Section 1.4(a): military plans, weapons systems, or operations
- Section 1.4(b): foreign government information
- Section 1.4(c): intelligence activities (including covert action), intelligence sources or methods, or cryptology
- Section 1.4(d): foreign relations or foreign activities of the United States, including confidential sources
- Section 1.4(e): scientific, technological, or economic matters relating to the national security
- Section 1.4(f): United States Government programs for safeguarding nuclear materials or facilities
- Section 1.4(g): vulnerabilities or capabilities of systems, installation, infrastructures, projects, plans or protection services relating to the national security; or
- Section 1.4(h): the development, production, or use of weapons of mass destruction

2. **Classification by Compilation**. A compilation of unclassified information is normally not classified. However, in certain circumstances, information that would otherwise be marked unclassified may become classified when combined or associated with other unclassified information, if the compiled information reveals an additional association or relationship that meets the standards and criteria for classification. Under such circumstances, it is the additional association or relationship revealed by the combination or compilation of information that is classified, not the individual items of information. Careful consideration must be applied when determining the need for classification by compilation. When the determination is made that the classification by compilation is necessary, the OCA must provide explicit instructions regarding what element of the compilation, when combined, constitutes classification and the additional associations or relationship that warrants the classification. Users of this Security Classification Guide should be aware of such a possibility when compiling unclassified information (see Paragraph 17.13 B.4 below).

   Likewise, the compilation of NSI will be classified, at a minimum, at the highest classification within the aggregated data but may become a higher classification if the compiled information reveals an additional association or relationship that warrants a higher level of classification (see Paragraph 17.13.B.4 below).

3. **Exceptional Circumstances**. Should a situation arise where a holder of information believes the information should be classified but it is not covered by this classification guide, or a compilation of unclassified information should be classified or, if already classified, classified at a higher level, the information will be handled and safeguarded in accordance with the level of classification that the

holder believes it to be. In such instances, the information will be marked with the tentative level of classification and the notation "Pending Classification Review."

4. **Challenges to Classification**. If, at any time, security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until a formal decision by an appropriate authority is made. Classification challenges should be addressed to OSY. Appellate procedures for classification determinations are found in 32 CFR Part 2001/2004, "Classified National Security Information," Directive No. 1, Final Rule.

5. **Use of This Guide**. This guide is for the use of Department employees performing original classification actions when addressing elements of information covered by this guide.

   For the purpose of marking documents containing NSI covered by this guide, original classification will cite, Commerce SCG, dated _____ 2008, on the "Classified By" line, followed by the name and title of the OCA and declassification instructions as specified in the guide. For example:

   Classified By: DOC SCG, _____ 2008
   Reason: E.O.13526
   Declassify On: 15 December 2020

   If NSI covered by this guide, as well as NSI from other classified sources, is included in the same document, the document will be marked as follows:

   Derived From: Multiple Sources
   Declassify On: (Carry forward the single most restrictive declassification instruction from all source documents. Specifically, carry forward the single declassification instruction that provides the longest protective time period.)

   Note: If "Multiple Sources" are used for a derivatively classified document, a record of the sources used should be maintained with the file copy of the document.

   When the declassification instruction of the source(s) is marked "OADR" or "Originating Agency Determination Required," or the declassification instruction from the source(s) cites X-1 through X-8, the declassification instructions for the newly created document will state: "Source Marked OADR," followed by the date of the most recent source; or "Source Marked X (applicable exemption number)" followed by the date of the most recent source. For example:

   Derived From: Multiple Sources
   Declassify On: September 22, 2028

   Note: If a source document is dated before 2003, add 25 years to the source document origination date. For example:

Derived From: Memorandum dated September 21, 2002
Declassify On: September 21, 2027

6. **Classified Processing**. NSI will not be processed on any automated information technology equipment unless the equipment has been specifically accredited and approved for classified processing. Consult the Office of Chief Information Officer for instructions on what equipment may be used.

7. **Marking**. Detailed instruction for marking classified materials can be found in Chapter 19, Marking of Classified National Security Information. Training on marking classified materials can be obtained by contacting the OSY Counterespionage Division, Information Security Branch, at (202) 482-8115. The ISOO Marking Pamphlet is available for download at http://www.archives.gov/isoo/index.html.

8. **Reproduction and Dissemination**. This guide may be reproduced and disseminated within the Department as needed. However, to ensure receipt of updates, revision, and classification changes whenever the guide is disseminated beyond the initial addressee, notify the OPR. Dissemination to Government agencies outside the Department must be coordinated through the OPR.

C. Public Release of Information.

The fact that this guide indicated that some information may be unclassified does not imply that the information is automatically releasable to the public. Request for public release of information will be processed in accordance with the Freedom of Information Act compliance.

Classification guides created by OCAs should be marked as "FOUO" [For Official Use Only] and will not be released to the public. Requests for copies of this guide by non-governmental officials will be processed under the Freedom of Information Act.

D. Defunct Organizations.

1. All NSI originated by the following defunct agencies whose functions were transferred to the Department may be declassified by using this authority:
   - Civilian Production Administration (1945–1946)
   - Office of Price Administration (1941–1946)
   - Office of Temporary Controls (1946–1947)
   - Office of War Mobilization and Reconversion (1944–1946)
   - United States Maritime Commission (1936–1950)
   - War Production Board (1942–1945)
   - War Shipping Administration (1942–1946)

2. For information on other defunct agencies whose functions have been transferred in whole or part to the Department and whose NSI may be declassified under these guidelines, see Appendix A of the current http://www.archives.gov/press/press-releases/2010/nr10-22.html.

Chapter 18. Declassification and Downgrading

18.1. DECLASSIFICATION

A. Information that continues to meet the classification requirements of Executive Order (E.O.) 13526, Classified National Security Information, requires continued protection; however, Department of Commerce (Department) information shall be declassified as soon as it no longer meets the standards for classification under this E.O. In some exceptional cases, the need to protect such information may be outweighed by the public interest to disclose the information, in which case the information should be declassified. When such questions arise, the Classified National Security Information (NSI) will be reviewed by the official who authorized the original classification if that official is still serving in the same position, by a successor, or by the Director for Security (Director) to determine, as an exercise in discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not do either of the following:

1. Amplify or modify the substantive criteria or procedures for classification.
2. Create any substantive or procedural rights subject to judicial review.

B. Information marked with a specific declassification date or event shall be declassified on that date or upon occurrence of that event. The overall classification markings shall be lined through and a statement placed on the cover or first page to indicate the declassification authority by name and title, and the date of declassification. The classification markings on each page also shall be lined through.

C. When declassification action is taken earlier than originally scheduled or the duration of classification is extended, the authority making such changes shall promptly notify all holders to whom the information was originally transmitted. This notification shall include the marking action to be taken, the authority for the change (name and title), and the effective date of the change. Upon receipt of notification, recipients shall make the proper changes and notify holders to whom they have transmitted the NSI.

D. If the Director of the Information Security Oversight Office (ISOO) determines that information classified by any operating unit in the Department is classified in violation of E.O. 13526, the ISOO Director may require that the information be declassified. Any such decision by the ISOO Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information will remain classified pending a decision on the appeal.

E. To the extent practicable, operating units of the Department shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified, in accordance with the provisions for automatic declassification sections of E.O. 13526.

F. Subject to Section 3-3 paragraphs (b)-(d) and (g)-(i) of E.O. 13526, all classified records that (1) are more than 25 years old and, (2) have been determined to have permanent

historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in paragraphs (b)-(d) and (g)-(j) of this section. If the date or origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

G. The Office of Security (OSY) shall cooperate with the National Archives and Records Administration (NARA) in developing schedules for the declassification of records in the National Archives of the United States and the Presidential libraries to ensure that declassification is accomplished in a timely manner. NARA will provide information about the records proposed for automatic declassification. Operating units shall consult with OSY and the Department's Records Management Officer before reviewing records in their holdings to ensure that appropriate procedures are established for maintaining the integrity of the records and that NARA receives accurate information about operating unit declassification actions when records are transferred to NARA. NARA will provide guidance to the Department's Records Management Officer concerning the requirements for notification of declassification actions on transferred records, box labeling, and identifying exempt information in the records.

18.2. DOWNGRADING

Information designated at a particular level of classification may be assigned a lower classification level by the original classifier or by an official authorized to declassify the same information. Prompt notice of such downgrading must be provided to known holders of the information. NSI marked for automatic downgrading under previous E.O.s should be reviewed to determine that it no longer continues to meet classification requirements despite the passage of time.

18.3. TRANSFERRED INFORMATION

A. When classified records are transferred from another agency or operating unit in conjunction with a transfer of functions, and not merely for storage purposes, the receiving operating unit shall be deemed the originating office for purposes of downgrading and declassification.

B. When classified records have not been officially transferred in conjunction with a transfer of functions but originated in an agency or operating unit in the Department that has ceased to exist and for which there is no successor office, the operating unit in possession of the classified records shall be deemed the originating office for purposes of the E.O. Such records may be declassified or downgraded by the operating unit that has possession of the documents after consultation with any other agency or unit that has an interest in the subject matter of the records.

C. When an operating unit discovers classified records originated by another agency, operating unit, or office that appears to meet the criteria for the application of the automatic declassification provisions of E.O. 13526, the finding unit should alert the

originating agency and seek instructions regarding the handling and disposition of pertinent records.

D. The originating operating unit or Departmental office shall take all reasonable steps to declassify information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records being transferred to the Archivist pursuant to 44 U.S.C. § 2203, records for which NARA serves as the custodian, or the records of an agency or organization that goes out of existence.

18.4. AUTOMATIC DECLASSIFICATION

A. NSI contained in records more than 25 years old that has been determined to have permanent historical value under Title 44 U.S.C. and does not meet the exemption standards noted below, shall be automatically declassified whether or not the records have been reviewed.

B. NSI may be exempted from automatic declassification when it might be expected to have any of the following characteristics:

1. Reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.
2. Reveal information that would assist in the development, production, or use of weapons of mass destruction.
3. Reveal information that would impair United States (U.S.) cryptology systems or activities.
4. Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system.
5. Reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans.
6. Reveal information, including foreign government information that would cause serious harm to relations between the U.S. and a foreign government, or to ongoing diplomatic activities of the U.S.
7. Reveal information that would 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.

8. Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security.

9. Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

C. If an operating unit proposes to exempt a specific file series of records from automatic declassification based on the exemptions listed in Paragraph 18.4.B, the head of the operating unit shall submit the information noted below to the Director for an assessment. After an evaluation, the Director or delegated representative will forward the request to the ISOO for action. The request should include all of the following:

1. A description of the file series.

2. An explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time.

3. Except when the information within the file series almost invariably identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, a specific date or event for declassification of the information, not to exceed December 31 of the year that is 50 years from the date of origin of the records.

D. Classified records within an integral file block, as defined in E.O. 13526, that are otherwise subject to automatic declassification shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

E. The Director may delay from automatic declassification the records noted below by notifying the Director of the ISOO. To obtain a delay, the head of an operating unit must submit a request to the Director at least 180 days before records in such a file series are subject to automatic declassification. The information noted in Paragraph 18.4.C. must be provided.

1. For NSI contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly, the Director may delay automatic declassification of records in a particular file series for up to five additional years.

2. For classified records subject to automatic declassification that have been referred or transferred to an operating unit by another agency less than three years before automatic declassification would otherwise be required, the Director may delay automatic declassification for up to three years.

3. For classified records that were inadvertently not reviewed prior to the effective date of automatic declassification, the Director may delay automatic declassification for up to three years from the date of discovery.

F. NSI exempted from automatic declassification under this chapter shall remain subject to the mandatory and systematic review provisions of E.O. 13526.

G. The Secretary of State shall determine when the U.S. should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section of the Manual of Security Policies and Procedures (Manual) for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

18.5. EQUITY REFERRALS

A. Records containing information or equities that originated with other agencies and the disclosure of which would affect the interests or activities of other agencies shall be referred for review to those agencies, and the information of concern shall be subject to automatic declassification only by those agencies, as defined in E.O. 13526.

B. For equity referrals within the Department, the bureau initiating the referral must contact the Original Classification Authority (OCA) of the bureau in writing with a courtesy copy to the Senior Agency Official. The receiving bureau shall make a prompt declassification decision within 30 days of receipt and notify the sender of its decision.

C. For information stored in security containers within the Department, subject to automatic declassification and still required for operational necessity, bureaus may send referrals directly to the agency in accordance with procedures established by the agency to which the information is referred. Department operating units may contact OSY for assistance. NARA standard referral procedures should be followed for records accessioned and processed. The Interagency Referral Center (IRC) is referenced in Paragraph 8.5.E.

D. Referrals to the Department from an outside agency not processed through the IRC can be made to the Director, OSY, Room 1067, 14th & Constitution Avenue, NW, Washington, DC 20230. NARA standard referral procedures should be followed for records accessioned and processed therein. The IRC is referenced in Paragraph 8.5.E.

E. The IRC is located at the NARA building, Room 3700 in College Park, Maryland 20740. A minimum Top Secret and/or "Q" clearance is needed to conduct reviews in the IRC. The IRC is one of the central locations where agencies can review records subject to automatic declassification, whether to declassify, exempt, exclude, or make equity referral decisions. NARA serves as the primary office for notifying agencies of equity referrals contained in the IRC.

1. For referrals to the Department from an outside agency, each bureau will be required to identify two potential reviewers to conduct reviews in the IRC.
2. For referrals from the Department to an outside agency, referrals will be processed using NARA-directed guidelines.

18.6. DECLASSIFICATION GUIDES

A. Approved declassification guides may be used as a tool to assist in exempting classified records from the automatic declassification provisions of E.O. 13526. These guides must include additional pertinent detail relating to the exemptions described in Paragraph 18.4 and follow the format required for declassification guides for systematic review as described in the Implementing Directive for E.O.13526. (32 CFR Part 2001), as amended. In order for such guides to be used in place of the identification of specific information within individual documents, the information to be exempted must be narrowly defined, with sufficient specificity to allow the user to identify the information with precision. Exemptions for general categories of information will not be acceptable. The actual items to be exempted are specific documents. All such declassification guides used in conjunction with automatic declassification provisions of E.O. 13526 must be submitted to the Director of ISOO, serving as Executive Secretary of the Interagency Security Classification Appeals Panel (ISCAP), for approval by the Panel.

B. Operating units shall prepare declassification guides to facilitate the declassification of information contained in records determined to be of permanent historical value. Declassification guides shall do all of the following:

1. Identify the subject matter of the declassification guide.
2. Identify the original declassification authority by name or personal identifier and position.
3. Provide the date of issuance or last review.
4. State precisely the categories or elements of information to be declassified, downgraded, or not declassified.
5. Identify any related file series that has been exempted from automatic declassification pursuant to E.O. 13526.

C. To the extent a guide is used in conjunction with the automatic declassification provisions of E.O. 13526, the guide shall state precisely the elements of information to be exempted from declassification, including both of the following:

1. The appropriate exemption noted in Paragraph 18.4, (when citing exemption category 9, list the applicable statute, treaty, or international agreement).
2. A date or event for declassification.

D. Operating units shall submit declassification guides for review to OSY Counterespionage Division (CED). To the extent such guides are used in conjunction with the automatic declassification provisions of E.O. 13526, OSY shall submit bureau-specific declassification guides to the ISCAP for approval.

E. Declassification guides shall be reviewed and updated as circumstances require but at least once every five years. Servicing Security Offices (SSOs) shall maintain a list of declassification guides in use and provide a copy to OSY CED.

18.7. SYSTEMATIC DECLASSIFICATION REVIEW

A. Each operating unit that has originated NSI under E.O. 13526 or its predecessors shall establish and conduct a program for systematic declassification review for records of permanent historical value exempted from automatic declassification under section 3.3 of the order, and this Manual. Operating units shall prioritize the systematic review of records based on the degree of researcher interest and the likelihood of declassification upon review.

B. Operating units or offices shall maintain a current listing of officials delegated declassification authority by name, position, or other identifier and shall provide the list to their SSO and OSY CED. If possible, this listing shall be unclassified.

1. An executive who has been delegated OCA may authorize an official in his or her operating unit to exercise declassification and downgrading authority regarding information classified during his or her tenure, by predecessors in that position, or for NSI transferred to that official's custody by virtue of a transfer of functions.
2. Unlike the OCA, which cannot be reassigned, the declassification authority may be reassigned as necessary. Each OCA shall forward a list of the names and position titles of those individuals receiving additional delegations to the bureau SSO, who will forward that list to OSY CED.

18.8. MANDATORY DECLASSIFICATION REVIEW

A. All information classified by an OCA in the Department under E.O. 13526, or its predecessor orders, is subject to a review for declassification if all of the following is true:

1. Request for a review describes the document or material containing the information with sufficient specificity to enable the operating unit or office to locate it with a reasonable amount of effort.
2. 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;
3. Information is not the subject of pending litigation.

B. Operating units or offices conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under E.O. 13526. The unit shall release this information unless withholding is otherwise authorized and warranted under applicable law.

18.9. PROCESSING REQUESTS AND REVIEWS

A. U.S. Originated Information.

1. In response to a request for information under the Freedom of Information Act (FOIA), or the mandatory review provisions of E.O. 13526, request for mandatory

review of NSI shall be submitted in writing and describe the information with sufficient specificity to locate it with a reasonable amount of effort. Requests shall be submitted through the OSY Strategic and Administrative Management Division, c/o the Counterespionage Division, 1401 Constitution Avenue, NW, Room 1521, Washington, D.C. 20230.

2. OSY shall directly inform the requester of its receipt of the request. The request will be forwarded to the operating unit or office that originated the information or that has primary interest in the subject matter. The operating unit or office must ensure the information is reviewed within 30 calendar days.

3. A valid mandatory declassification review request need not identify the requested information by date or title of the responsive records but must be of sufficient specificity to allow the operating unit or office with primary interest to locate the records containing the information sought with a reasonable amount of effort. In responding to mandatory declassification review requests, the designated official shall either make a prompt declassification determination (within 30 calendar days) and process the request accordingly or inform OSY of the additional time needed to process the request. When information cannot be declassified in its entirety, operating units will make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Upon denial of an initial request, OSY shall notify the requester of the right of an administrative appeal. This request must be filed within 60 calendar days of receipt of the denial.

B. Requests for Classified Records in the Custody of the Department Other than the Originating Office. When the Department receives a mandatory declassification review request for records in its possession that were originated by another agency, OSY CED shall refer the request and the pertinent records to the originating agency. However, if the originating agency has previously agreed that the custodial operating unit may review its records, the custodial operating unit shall review the requested records in accordance with declassification guides or guidelines provided by the originating agency. Upon receipt of a request from the referring agency, OSY shall process the request in accordance with this chapter. The originating agency shall communicate its declassification determination to the referring agency.

C. Appeals of Denials of Mandatory Declassification Review Requests. Following the receipt of an appeal, the Director shall normally make a determination within 60 calendar days. If additional time is required to make a determination, the Director shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The Director shall notify the requester in writing of the final determination and of the reasons for any denial.

D. Appeals to the Interagency Security Classification Appeals Panel. Requesters have the right to appeal the decision of the Director to the ISCAP in accordance with E.O. 13526.

E. Foreign Government Information.

1. When foreign government information is being considered for declassification or is subject to mandatory declassification, the declassifying unit shall determine whether the information is subject to any exemptions that would prevent its declassification at that time. Depending on the date of the information and whether it is contained in permanently historical records, the declassifying unit shall also determine whether other exemptions that pertain to U.S. foreign relations may apply to the information. If the declassifying unit believes such an exemption may apply, it should consult with all other concerned agencies in making its declassification determination.

2. The Department of State shall determine when the U.S. should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by the automatic declassification provisions of E.O. 13526, for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years.

F. Cryptologic and Intelligence Information. Mandatory declassification review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in accordance with special procedures issued by the Secretary of Defense and the Director of National Intelligence, respectively.

G. Fees. In responding to mandatory declassification review requests for classified records, agency heads may charge fees in accordance with section 483a of Title 31 U.S.C. (31 U.S.C. § 483a). Operating units should contact the Department's FOIA/Privacy Act Officer for the current schedule of fees.

H. Assistance to the Department of State. Operating units and the Department's Records Management Officer should assist the Department of State in its preparation of the Foreign Relations of the United States (FRUS) series by facilitating access to appropriate classified materials in its custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

I. Requests Filed Under Mandatory Declassification Review and the Freedom of Information Act (FOIA). When a requester submits a request under both mandatory review and the FOIA, OSY shall require the requester to elect one process or the other. If the requester fails to elect one or the other, the request will be treated as a FOIA request unless the requested materials are subject only to mandatory review.

J. FOIA and Privacy Act Requests. The Office of General Counsel shall ensure that requests for declassification submitted under the provisions of FOIA, as amended, or the Privacy Act of 1974 (PA), are processed in accordance with the provisions of those acts.

1. FOIA and the PA authorize withholding from public availability records that are properly classified under criteria established by E.O. 13526, in the interest of national defense or foreign policy.
2. Under FOIA, a determination on an initial request must be made within 20 working days after receipt of the request. A determination on an appeal to an initial denial must be made within 20 working days after receipt of a FOIA appeal, or for a PA appeal, within 30 working days. Time limits are mandatory for a FOIA request but are permissive for a PA request. Except for unusual circumstances, failure to make a determination within the stated time limits means that a requester has exhausted the administrative remedies and may request judicial review immediately.
3. To assure that FOIA and PA requests involving classified records are subjected to a thorough classification review and that a response is made within the specified time limits, the following procedures shall apply:
   a. The office of primary interest shall conduct a mandatory declassification review of the information.
   b. If the information is subsequently declassified, the action office must consult with the Office of the Assistant General Counsel for Administration to determine releasability with consideration only for the legality of release within the purview of FOIA and PA.
   c. If the record warrants continued classification, the action office must coordinate with the Office of the Assistant General Counsel for Administration and advise the requester of the decision and of the right of appeal.
4. Appeals for reconsideration of denial of a classified record under the FOIA shall be processed as follows.
   a. Appeals under this section must be addressed to the Assistant General Counsel for Administration who shall refer the record(s) to the Director for a declassification review. The Director may overrule previous determinations in whole or in part when, in his or her judgment, continued protection in the interest of national security is no longer required.
   b. If the information under review no longer requires classification, it should be declassified. The Director shall advise the Assistant General Counsel for Administration of the decision.
   c. Persons who request information under the provisions of FOIA or PA, and whose requests are denied on appeal, may petition the courts to direct the Department to release the information. Under judicial review, the Department must provide sufficient justification to continue withholding the information.

K. Redaction Standard. Operating units or offices are encouraged but are not required to redact documents that contain information that is exempt from the mandatory declassification provisions of E.O. 13526, especially if the information that must remain classified comprises a relatively small portion of the document. Operating units shall

redact documents that are the subject of an access request unless the overall meaning or informational value of the document is clearly distorted by redaction.

Chapter 19. Marking of Classified National Security Information

19.1. Marking Standards

A uniform security classification system requires that standard markings be applied to Classified National Security Information (NSI). Except in extraordinary circumstances, or as approved by the Director of the Interagency Security Oversight Office (ISOO), the marking of NSI created after October 14, 1995, and modified September 22, 2003, shall not deviate from the prescribed formats indicated in Paragraph 19.2. The Department of Commerce (Department) National Security Classification Guide (see Chapter 17, Security Classification) prescribes the markings that shall be uniformly and conspicuously applied to ensure the classified status of the information, the level of protection required, and the duration of the classification.

19.2. Marking of Classification Level

A. Overall Markings. Documents shall be marked with the highest classification level (Top Secret, Secret, or Confidential) of information contained in the document. The markings shall be printed or stamped in bold letters at the top and bottom of the outside front cover (if there is one), on the title page (if there is one), on the first page, and on the outside back cover (if there is one).

B. Page Markings. Each interior page is typed or stamped at the top and bottom according to the highest classification of the contents of the page, including the designation Unclassified, when appropriate, or according to the overall classification of the document. The three authorized classification designations (Top Secret, Secret, or Confidential) may be used in conjunction with approved Intelligence Community compartmented information code words.

C. Portion Marking.

1. Each subject line, title, paragraph, subparagraph, section (e.g., classified diagram, map, drawing, etc.) or similar portion of a classified document shall be marked to show the level of classification of that portion or to indicate that it is unclassified. Classification of portions of a document must be shown by placing the appropriate classification symbol immediately before or after the portion. In marking portions, the parenthetical symbols "TS" for Top Secret, "S" for Secret, "C" for Confidential, and "U" for Unclassified will be used. Classified and unclassified subjects and titles will be marked with the appropriate symbol placed immediately following or to the right of the subject or title. An unclassified short title will be used for reference purposes.

2. The Director of ISOO may grant and revoke waivers of the foregoing portion marking requirement. A request for such a waiver must be made through the Director for Security (Director) to the Director of ISOO. The written request must identify the information or class of documents for which the waiver is sought and a declaration that the circulation of the document and its potential as a source for derivative classification determinations will be kept to a minimum. The increased administrative burden of portion marking may not be used as the sole justification for the waiver.

3. When elements of information in one portion require a different classification but segregation into separate portions would destroy continuity or context, the highest classification required for any element to that portion shall be used.

19.3. ORIGINAL CLASSIFICATION PRIMARY MARKINGS

Required Markings. At the time of original classification, primary markings should be applied as outlined in Chapter 17, Security Classification, of this Manual of Security Policies and Procedures (Manual).

19.4. DURATION OF CLASSIFICATION

A. At the time of original classification, the Original Classification Authority (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 or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the date or event shall not exceed the time frame established in E.O. 13526.

B. If the OCA cannot determine an earlier specific date or 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.

C. An OCA may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under E.O. 13526 are followed.

D. No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination Required," or NSI that contains incomplete declassification instructions or lacks declassification instructions shall be declassified in accordance with part three of this order.

19.5. DERIVATIVE CLASSIFICATION MARKINGS

A. Required Markings. When a classified source document is used as the basis for derivative classification, the markings on the source document determine the markings to be applied to the derivative document. Persons who apply derivative classification markings shall be identified by name and position, or by personal identifier, in a manner which is immediately apparent for each derivative classification action.

1. **"Derived From" line:** Derivative classifiers shall identify the title and date of the classification guidance used (source document or classification guide). If more than one source document, classification guide, or combination of the two is used, the line shall read "**Multiple Sources**". If "Multiple Sources" is used, each source used shall be identified on a list maintained with the file or record copy of the document.

2. **"Declassify On" line:** Derivative classifiers shall carry forward the date of declassification specified by the original classifier or use the declassification instructions contained in the classification guide from which the classification was derived.

   a. When deriving from multiple source documents, the "Declassify On" line shall reflect the longest duration of any of the sources.
   b. When deriving from a source document marked with the declassification instruction "Originating Agency's Determination Required" (OADR) or a declassification instruction that contains any of the exemption markings X1 through X8, the derivative classifier shall carry forward the fact the source document(s) was marked with this instruction and the date of the origin of the most recent source document(s). See example 19.5.C.4 and 19.5.C.5.

B. Duration of Classification. For information marked "Originating Agency's Determination Required," its acronym OADR, or with some other marking indicating an indefinite duration under a prior order, the duration of the classification status may be limited as follows.

1. A declassification authority may declassify the information after gaining the consent of the original classifier.
2. An executive with OCA who has jurisdiction over the information may re-mark the information to establish duration of classification consistent with requirements of the original classification.
3. Unless declassified earlier, the information contained in historical records determined to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to automatic declassification provisions of E.O.13526.

C. Derivative Classification Block Examples.

1. The Department of Commerce National Security Classification Guide with a January 1, 2010, declassification date:

Classified by:	**Full Name & Title**
Derived From:	U.S. DOC Classification Guide, dated January 1, 2000
Declassify On:	January 1, 2010

2. A single reference (source) from the Department of State with a January 1, 2009, declassification date:

Classified by:	**Full Name & Title**
Derived From:	Memorandum subject title and date of the memorandum
Declassify On:	January 1, 2009

3. Information from several sources or references:

*When using multiple sources, list those sources and attach to the official file copy.

Classified by:	**Full Name & Title**
Derived From:	Multiple Sources*
Declassify On:	Use longest declassification duration from multiple sources.

4. The source document has OADR for the declassification instruction:

Classified by:	**Full Name & Title**
Derived From:	DIA Report dated 20 October 1989 Subject: New Weapons
Declassified On:	Source marked OADR, date of source: 20 October 1989

5. The source document has X, along with one or more of the categories numbers from 1–8:

Classified by:	**Full Name & Title**
Derived From:	DIA Report dated 25 October 2002
Declassify On:	Source marked X1, date of source: 25 October 2002

19.6. DOWNGRADING

When the classification level of a document is to be downgraded automatically, a notation to that effect must be printed or stamped on the face of the document as follows.

Downgrade To:	(classification) **on** (date or event)
Abbreviation:	DNG (classification) **on** (date or event)

19.7. CHANGES IN CLASSIFICATION MARKINGS

Whenever NSI is downgraded or declassified, or the initial classification changes, the information should be marked to reflect the change as well as the authority for and date of the action. However, when the volume of information is such that re-marking each classified item would interfere with operations, the custodian can attach downgrading, declassification, or upgrading notices to the storage unit. The notice should indicate the change, the authority for the action, the date of the action, the identity of the person taking the action, and the storage units to which it applies. When individual documents or other materials are withdrawn from such storage units, they should be promptly re-marked or have the old markings canceled.

19.8. TRANSMITTAL DOCUMENTS

A. Unclassified Transmittal Documents. A transmittal document that does not contain NSI shall be marked with the highest level of classification of the attachments. The

classification markings should appear at the top and bottom of the first page of the transmittal document, and the following marking shall be placed at the bottom of the transmittal page as follows:

"Unclassified when separated from classified attachments."

B. Classified Transmittal Document. Transmittal documents containing NSI must be marked on the top and bottom with the highest classification of the information contained in the transmittal or the attachments. If the information contained in the attachment is classified at a higher level than the transmittal itself, the transmittal document shall be marked as follows:

1. Secret transmittal with Top Secret attachment:

   "Secret when separated from classified attachment."

2. Confidential transmittal with Secret attachment:

   "Confidential when separated from classified attachment."

3. The transmittal must also be portion marked as prescribed for other classified documents.

19.9. OTHER MARKINGS

A. Foreign Government Information.

1. Documents that contain foreign government information shall be marked:

   "This Document Contains [indicate country of origin] Information."

2. The portions of the document that contain the foreign government information shall be marked to indicate the government and classification level (i.e., "UK-C").

3. If the specific foreign government must be concealed, the documents shall be marked:

   "This Document Contains Foreign Government Information."

   and pertinent portions shall be marked "FGI" (meaning "Foreign Government Information") together with the classification level (i.e., "FGI-C"). In such cases, a separate record that identifies the foreign government shall be maintained to facilitate subsequent declassification actions.

4. If foreign government information must be concealed, the markings should not be used. The document should then be marked as if it were of U.S. origin.

5. When classified records are transferred to the National Archives and Records Administration for storage and archival purposes, the accompanying documentation shall identify the portions that contain foreign government information. See Chapter 21, Transmission of Classified National Security Information, for safeguarding and transporting procedures.

6. Documents need not be re-marked as foreign government information when they bear foreign government or international organization markings such as "NATO."

7. When foreign government information is being considered for declassification or appears to be subject to automatic declassification, ordinarily the declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

B. Intelligence Sources or Methods. For NSI relating to intelligence sources or methods, apply the marking:

"WARNING NOTICE—Intelligence Sources or Methods Involved," (WNINTEL).

Information bearing this marking shall not be disseminated in any manner to employees who do not have a need to know as determined by the Servicing Security Officer (SSO) from the Office for Security.

C. Restricted Data (RD). For NSI containing RD, as defined in Section 142 d. of the Atomic Energy Act of 1954, as amended (42 U.S.C. § 2162, 2163, 2168, and 7383), the following shall be marked:

RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to Administrative and Criminal Sanctions.

D. Formerly Restricted Data. For NSI containing Formerly Restricted Data (FRD), as defined in Section 142 d. of the Atomic Energy Act of 1954, as amended (42 U.S.C. § 2162, 2163, 2168, and 7383), the following shall be marked:

FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to
Administrative and Criminal Sanctions.
Handle as Restricted Data in Foreign Dissemination Section 144.b.,
Atomic Energy Act, 1954.

E. Special Notations. Any appropriate notations (e.g., special handling requirements, dissemination limitations, etc.) shall be noted on the face of the document. Common notations are illustrated below:

1. **Not Releasable to Foreign Nationals (NOFORN).** This marking is used with a security classification to identify intelligence information that may not be released in any form to foreign governments, foreign nationals, or non-U.S. citizens without the permission of the originator.

2. **Not Releasable to Contractors/Consultants (NOCONTRACT).** This marking is used with a security classification to prohibit the dissemination of intelligence information to contractors or consultants without the permission of the originator.

3. **Dissemination and Extraction of Information Controlled by Originator (ORCON).** This marking is used with a security classification to enable the originator to supervise the use of the information.

19.10. TELEGRAMS AND CABLES

A. Printed copies of electrically transmitted telegrams and cables that contain NSI shall be marked at the top and bottom of the page with the assigned classification. Portion markings shall be applied also. When a telegram or cable is printed by an automated system, the classification markings can be applied by that system provided the markings are clearly distinguishable from the printed text. All required classification blocks for original or derivative classification authority must be listed on the telegram using abbreviations prescribed in this chapter.

B. Outgoing electrically transmitted classified telegrams and cables that contain information requiring original classification must be approved by an individual designated as an OCA prior to transmitting. The transmission date of the document will be considered to be the date of classification.

19.11. FILES, FOLDERS, AND BINDERS

Classified cover sheets, SF-703 (Top Secret), SF-704 (Secret), or SF-705 (Confidential), shall be affixed to the exterior cover of files, folders, and binders that contain NSI. Each standard form shall be used according to the highest classification of the contents. Classified cover sheets shall be affixed to classified documents when stored in a storage container, upon receipt of a document that may be without one, and at any time a classified document is handled. The only occasion when a cover sheet does not need to be affixed to an individual document is when the document is placed in a folder or binder with other classified documents where the appropriate cover sheet is affixed to the exterior cover to identify the highest level of the documents contained within a folder or binder. Files and folders shall be marked or stamped with the highest level of classified material contained in the folder. Binders shall have the appropriate classified cover sheet attached to the binder.

19.12. OTHER MATERIALS

Security classification and declassification instructions must be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal, or similar device on classified material other than paper copies of documents. If marking the material or container is not practicable, written notification of the security classification and declassification instructions shall be furnished to recipients. The following procedures for marking various kinds of material containing NSI are not all-inclusive and shall vary to accommodate the physical characteristics of the material containing the NSI. Safes and other security containers, which are routinely used to store classified documents, shall not bear a classification marking.

A. Charts, Maps, Graphs, and Drawings. Charts, maps, graphs, and drawings must bear the appropriate overall classification marking under the legend, title block, or scale. Portion marking shall be used to indicate the highest level of classification of the legend or title itself. The highest level of classification shall be inscribed at the top and bottom of each document. When charts, maps, graphs, or drawings are folded or rolled, the classifier must apply additional markings that are clearly visible when the document is folded or rolled.

B. **Photographs, Films, and Recordings.** Photographs, films (including negatives), recordings, and their containers shall be marked to alert a recipient or viewer that the material contains NSI.

1. **Photographs.** Negatives and positives shall be marked whenever practicable with the appropriate classification level, authority, and declassification instructions. The classification level shall be marked at the beginning and end of each strip. All markings shall be placed on containers of negatives and positives. When self-processing film or paper is used to photograph or reproduce NSI, the classifier must remove all parts of the last exposure from the camera and destroy them as classified waste, or the camera should be protected as classified material. Prints and reproductions must be marked with the appropriate classification level, downgrading, if applicable, and declassification instructions on the face side of the print if possible. Markings that cannot be applied to the face side shall be stamped on the reverse side or affixed by pressure tape label, stapled strip, or other comparable means.

2. **Transparencies and Slides.** Classification markings shall be shown clearly on the image of each transparency or slide or on its border, holder, or frame.

3. **Motion Picture Films.** Classified motion picture films and videotapes shall be marked at the beginning and end of each reel with titles bearing the appropriate classification. Markings must be visible when projected. Reels must be kept in containers bearing conspicuous classification, declassification, and, if applicable, downgrading markings.

4. **Recordings.** Sound, magnetic, or electronic recordings shall contain a clear statement of the assigned classification level at the beginning and end. Recordings must be kept in containers or on reels that bear conspicuous classification, declassification, and, if applicable, downgrading markings.

5. **Microfilm or Microfiche.** Microfilm or microfiche contains images in sizes too small to be read by the unaided eye. Accordingly, the classification must be marked conspicuously on the microfilm medium or its container so it is readable by the unaided eye. In addition, these markings must be included on the image so that when the image is enlarged and displayed or printed, the markings are conspicuous and readable.

C. **Automated Information Technology (IT) Storage Media.** Storage media (e.g., hard drives, diskettes, floppies, etc.) that contain NSI shall bear external classification markings and internal notations indicating the classification level, authority, and declassification instructions. Exterior labels shall be used to mark magnetic or digital media, other non-paper media, and equipment for which use of cover sheets is not feasible. The following standard forms shall be affixed to each item, depending on the classification: SF-706 (Top Secret), SF-707 (Secret), SF-708 (Confidential), and SF-710 (Unclassified). SF-710s for unclassified media are required for use in controlled environments but are not required for unclassified media stored in uncontrolled office

space. All media stored in storage containers used for the storage of classified materials must have the appropriate level of label affixed.

D. Classified Documents Produced by IT Equipment. Each page produced by IT equipment authorized to process NSI shall bear classification markings.

E. Material Used for Training Purposes. Unclassified materials used to simulate classified documents or materials for training purposes shall be marked:

"[Classification] for training purposes only, otherwise Unclassified."

F. Classified Waste Materials. Materials such as rejected copies, computer disks, and similar items shall be handled in a manner that assures adequate protection of the NSI contained in the media. When the materials are no longer needed, they shall be destroyed by approved methods (see Chapter 33, Storage and Destruction Equipment).

G. Classified Working Papers. Classified working papers are drafts, notes, photographs, etc., used to create or assist in the preparation of a final classified document. They must be dated when created, marked with the highest level of classification contained within the document, and destroyed when no longer needed. When any of the following conditions apply, working papers will be controlled and marked in the same manner for a finished document:

1. Released by the originator outside the originating activity
2. Retained more than 180 days from the date of origin
3. Filed permanently

H. Special Access Program Materials. Additional markings, as prescribed in directives, regulations, and instructions related to any applicable special access program, shall be applied to materials containing information protected by a special access program. These additional markings should not serve as the sole basis for continuing classification of special access program information.

Chapter 20. Access and Dissemination of Classified National Security Information

20.1. Access to Classified National Security Information (NSI)

A. The heads of operating units must ensure that only authorized persons obtain access to NSI.

B. Access to NSI must be consistent with the policies and procedures outlined in Chapter 9, Personnel Security Policies, and Chapter 16, Classified National Security Information Policies, of this Manual of Security Policy and Procedures (Manual).

C. Employees approved for access to NSI must sign the Classified Information Nondisclosure Agreement, SF-312, after receiving an initial NSI briefing, the formal granting of a security clearance, and agree to be bound by statutes concerning the protection of NSI.

20.2. Termination of Access

A. Upon termination of a security clearance, the holder shall receive a formal security debriefing describing the continuing responsibility to protect the NSI to which the individual had access. Page two of the SF-312 shall be completed upon debriefing. In addition, a copy of the sanctions under Title 18, United States Code, Section 798 shall be given to the debriefed employee to reemphasize criminal prosecution penalties for unauthorized disclosure of NSI.

B. NSI (in any form), including extra copies, is not personal property and may not be removed from the Government's control by any departing employee or contractor. The operating unit Security Contact shall ensure that all debriefed personnel have accounted for all NSI in their possession and transferred it to an authorized custodian. The Servicing Security Office (SSO) shall verify that the departing individual does not have any classified documents or security containers still assigned to him or her.

20.3. Restrictions

A. NSI may only be discussed when all of the following four conditions are fulfilled:

1. Recipient of the NSI has a current security clearance at the appropriate level.
2. Holder of the NSI has verified the identification of the intended recipient.
3. Holder of the NSI has verified a need to know by the intended recipient.
4. Discussion must be held in appropriately cleared Federal Government or contractor facilities to preclude unauthorized disclosure of NSI. Contact the Office of Security (OSY) for any variance of this restriction.

B. NSI may not be removed from official premises without proper authorization. An official or employee leaving agency service may not remove NSI from Department of Commerce (Department) control.

C. NSI shall remain under the control of the originating agency or its successor in function. Operating units in the Department shall not disclose information originally classified by another agency without its authorization. Persons authorized to disseminate NSI outside the Executive Branch shall ensure the protection of the information in a manner equivalent to that provided within the Executive Branch.

D. Discussing NSI in homes, public places, on public conveyances, or anywhere unauthorized persons have access is strictly prohibited. Employees or other individuals cannot retain or use NSI for their private use.

E. Secure Telephone Equipment, and other National Security Agency approved secure telecommunications, as well as secure facsimile equipment must be used for the telephonic and data transmission of NSI. Specific questions regarding the use of the telecommunication systems for transmission of NSI should be directed to the Department's Communications Security Custodian in OSY. Standard telephones shall not be used for classified discussions.

F. Electronic processing and/or transmission of NSI on a computer can only be accomplished on the Secret Internet Protocol Network, the Joint Worldwide Intelligence Communications System, or an Office of Chief Information Officer accredited stand-alone computer dedicated to the processing of NSI.

G. Each operating unit in the Department shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the Government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Classified" information, including modified handling and transmission and allowing access to individuals with a need to know who have not otherwise been cleared for access to NSI or executed an approved nondisclosure agreement.

H. Except as otherwise provided by statute, Executive Order (E.O.) 13256, directives implementing this Order, or by direction of the President, NSI originating in one agency shall not be disseminated to another agency without the consent of the originating agency. The Director for Security (Director) may waive this requirement for specific information originated within that agency. Prior consent is not required when operating units refer records for declassification review that contain information originating in several agencies.

20.4. CERTIFICATION OF SECURITY CLEARANCE

Any employee, contractor, expert, or consultant of the Department who has a need to access another agency or facility must initiate the Visit Authorization and Clearance Certification Request, Form CD-414. The form must be completed, signed by the SSO, and submitted to the agency to be visited. The form shall be submitted within five working days of the visit, or period of clearance certification. However, some agencies or government facilities require the use of

their own form for visits to their facilities. The individual coordinating the clearance certification request should verify the method acceptable to other agencies prior to the visit.

20.5. Access by Historical Researchers and Former Presidential Appointees

A. Persons who are engaged in historical research projects or who have previously occupied policymaking positions appointed by the President may be granted authorized access to NSI provided the head of the operating unit with jurisdiction over the information executes all of the following steps:

1. Makes a written determination that access is consistent with the interests of national security and forwards a copy of this determination to the Director.
2. Takes appropriate steps to protect NSI from unauthorized disclosure or compromise and ensures that the information is safeguarded in a manner consistent with E.O. 13526 and this Manual.
3. Obtains written nondisclosure agreements from the requester to safeguard the information to which he or she is given access in accordance with this Manual.
4. Obtains written consent to a review by the Department of the requester's notes and manuscripts to determine that no NSI is contained in the material and/or to ensure NSI does not leave Department facilities.
5. Limits access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

B. Historical researchers and former Presidential appointees will provide the heads of Department operating units with a detailed description of their research. Access will be granted to these individuals for a limited period of time. Requests for access must be made in advance and approved by the Director. Access will be granted only if a compelling need exists and it is in the Department's best interest. The information requested shall be clearly identified so that it can be located and compiled with a reasonable amount of effort. If the access requested by an historical researcher or a former Presidential appointee requires the rendering of services for which fair and equitable fees may be charged, the requester shall be so notified.

C. The provisions of Section III, Classified National Security Information, of this Manual apply only to NSI originated by Department, or information that is now in the sole custody of the Department; otherwise, the researcher should be referred to the classifying agency. Operating units providing information in accordance with this section of this Manual must maintain custody of NSI at a Departmental facility or a facility approved by the Department to house NSI.

20.6. Access by Foreign Governments, International Organizations, and Non-U.S. Citizens

A. If the head of an operating unit indicates a need to provide access to non-U.S. citizens, the sponsoring officer must consult with the Director for a final decision.

B. Non-U.S. citizens employed by the Department who meet the requirements set forth in Chapter 11, Investigative Processing, may be granted access to NSI originated by the Department. Access shall be granted only for the specific classified project to which they are assigned and only after they have met the requirements set forth in this Manual, and as outlined in paragraph C.

C. Dissemination of classified military information to foreign governments and international organizations is governed by the National Disclosure Policy (NDP-1).

D. The Director shall approve any recommendation to release NSI to a foreign government or international organization.

20.7. DISSEMINATION OF DEPARTMENT NSI

A. The heads of all operating units, or their designee, are responsible for providing direct control of the dissemination of NSI received or generated in his or her offices.

B. The head of an office who hosts or convenes a meeting (i.e., conference, symposium, seminar, exhibit, convention, scientific, or technical gathering) at which NSI is disclosed must do all of the following:

1. Verify the security clearance and need to know of each person attending the meeting.
2. Identify attendees before admitting them to the meeting room.
3. Advise persons (i.e., speakers) who will present NSI of any limitations on their presentation that may be necessary because of the level of security clearance and need to know of the attendees. Speakers are responsible for seeking such guidance and for keeping classified disclosures within the prescribed limits. They are also responsible for advising the audience of the classification level of, the authority for, and the duration of the classification of the information disclosed, including any special marking, storage, or safeguarding requirements.

C. Employees who attend meetings where NSI is disclosed shall obtain adequate information on the level and duration of, and authority for, classification of the information disclosed in order to provide appropriate derivative classification to any documentation resulting from the meetings.

D. Notes, minutes, summaries, recordings, proceedings, reports, and so forth, of the classified portions of the meeting are referred to as working papers. The materials shall be safeguarded and controlled throughout the duration of the meeting. At the conclusion of the meeting, the materials shall be forwarded, if needed, to attendees by approved secure transmission methods. See Chapter 21, Transmission of Classified National Security Information, of this Manual for proper transmission of NSI.

E. Physical and technical security controls shall be established appropriate to the classification and sensitivity of the information to be discussed. Because of the inherent security threats, classified meetings or classified sessions of a meeting shall be held in

appropriately cleared Federal Government or contractor facilities to preclude unauthorized disclosure of NSI. Contact OSY for any variance of this restriction.

20.8. DISSEMINATION OF OTHER AGENCY INFORMATION

NSI originated in another agency shall be disseminated outside the Department only with the consent of the originator. This is commonly known as the "Third Agency Rule." Consent must be maintained in writing as a matter of record. This restriction does not apply to additional distribution within the Department or distribution to Department contractors who are U.S. citizens and require the information in performance of contracted services (unless the documents are marked "PROPIN" [Proprietary Information]).

20.9. DISSEMINATION OUTSIDE THE EXECUTIVE BRANCH

Department NSI can be made available to persons outside the Executive Branch provided: (1) they are engaged in historical research projects or previously have occupied policymaking positions and were appointed by the President; or (2) the information is necessary for their performance of a function related to a contract or other agreement with the Federal Government; or as provided below.

A. United States Congress.

1. NSI originated by the Department shall be released to the U.S. Congress, its committees, members, and staff representatives when necessary in the interests of the national security and as authorized by the Secretary of Commerce or the head of an operating unit. Such release shall coincide with the provisions of Department Administrative Order 218-1, Legislative Activities. Proposals to transmit NSI to the U.S. Congress must be reviewed by the SSO, the Director, and the Office of General Counsel, prior to release.
2. Department personnel who appear as witnesses before a Congressional committee shall request that classified testimony be given in executive session only, that any record of such testimony be identified as classified and not appear in any document subject to public inspection or availability, and shall obtain the assurance of the committee chair that everyone present has appropriate security clearances or agrees to safeguard the NSI from public disclosure. By virtue of their elected positions members of Congress are allowed access to NSI. However, staffs of members and committees must have an appropriate security clearance prior to gaining access to NSI. Security clearances of congressional staff must be verified through the operating unit's SSO and forwarded to OSY Counterespionage Division.
3. Individuals who release NSI shall assure that the designated security classification is still valid and that the recipient is advised of the need to protect the information from unauthorized disclosure.

B. General Accountability Office (GAO). Properly cleared and identified representatives of the GAO can be granted access to NSI originated by the Department when the

information is relevant to an ongoing GAO review or investigation. The security clearance of a GAO official shall be verified through OSY prior to release of the NSI.

C. Judiciary.

1. An employee, office, or operating unit receiving an order or subpoena issued by a Federal or state court of record to produce NSI shall immediately refer the order or subpoena to the appropriate General Counsel's office. NSI shall be subject to an "in camera" review by the judge of the court of record to determine the relevancy of the information in question.
2. If NSI is to be introduced as evidence, access must be limited to the presiding judge of the court and the attorneys and other persons whose duties require knowledge or possession of the information and who have been cleared in accordance with applicable regulations. In addition, the following safeguards must be followed.
   a. All proceedings must be held in a secure court or hearing room.
   b. Dissemination and accountability controls must be established for all NSI marked for identification or offered or introduced as evidence.
   c. The transcript of the proceeding must be properly marked to indicate the classified portions that must be segregated from unclassified portions and properly safeguarded and stored.
   d. Any classified notes, drafts, or other documents produced by non-Department individuals that are no longer required by any party to the proceeding, must be transferred to the Department for destruction.
   e. Each recipient of NSI disclosed under the provisions of Section III, Classified National Security Information, of this Manual shall be advised of the classification level, safeguard and storage requirements, and the liability in the event of unauthorized disclosure.
   f. At the conclusion of the proceeding all NSI shall be returned to the Department or placed under seal of the court of record.
   g. NSI shall not be introduced as evidence at a civil trial before a jury.

D. Industrial, Educational, and Commercial Entities. Certain bidders, contractors, grantees, or educational, scientific, or industrial organizations shall receive NSI only under the procedures prescribed by the National Industrial Security Program (NISP) (see Chapter 37, Industrial Security).

20.10. Dissemination Outside the Federal Government

A. NSI under the control of the Department shall be released outside the Federal Government to organizations such as state or municipal agencies, firms, corporations, educational institutions, private individuals, or other non-federal sources if both of the following conditions are satisfied:

1. Recipient is acting in a contractual or official capacity with the Department.

2. Recipient has a need to know the information to further the mission of the Department and has a national security clearance or is eligible for such access.

B. In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the Director may authorize the disclosure of NSI to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with the directives implementing E.O. 13526 and procedures described in this Manual governing the release of NSI. The disclosure of NSI under these circumstances and the number of individuals authorized access shall be minimized consistent with operational necessity. Information disclosed under this provision shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the NSI.

C. The employee releasing the information must verify the recipient's security clearance and facility clearance through the operating unit's Security Contact.

D. Any proposed releases of NSI outside the Department not specifically covered by this chapter shall be coordinated with OSY before release.

20.11. DISSEMINATION OF RESTRICTED AND FORMERLY RESTRICTED DATA

Information bearing the warning notices "Restricted Data" or "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and shall not be disseminated outside the Department without the consent of the originator. The originator of the "Restricted Data" or "Formerly Restricted Data" is the Department of Energy (see E.O. 13526).

Chapter 21. Transmission of Classified National Security Information

21.1. TRANSMITTAL OUTSIDE DEPARTMENTAL FACILITIES

A. All Classified National Security Information (NSI) transmitted outside a Department of Commerce (Department) facility shall be enclosed in an opaque inner and outer cover (e.g., sealed envelopes, wrappings, or a locked container) which conceals the contents and would reasonably be expected to indicate evidence of tampering. The inner sealed cover shall be clearly marked on both sides with the highest classification of the information contained within, any required protective markings, and complete forwarding and return addresses. The outer sealed opaque cover shall be addressed in the same manner but shall not bear any classification markings or other indication that NSI is enclosed. The following exceptions apply:

1. When the outside shell or body of an item of equipment contains an internal component that is classified, the shell may be considered the outer enclosure provided it does not reveal NSI.
2. When an internal component of a bulky item of equipment is classified but inaccessible, the outside, or body, of the item may be considered a sufficient enclosure provided that the internal component cannot be observed and the outer body does not reveal NSI.
3. When an item of equipment is classified but cannot reasonably be packaged and the shell or body of the equipment is classified also, the shell or body shall be concealed with an opaque enclosure that will hide all classified features.
4. Specialized shipping containers, including closed cargo transporters, may be considered the outer enclosure in applicable circumstances. The specialized shipping container must be secured with a high-security padlock and equipped with an electronic seal that would provide evidence of surreptitious entry. The container's construction must also be such that it would indicate evidence of forced entry. A specialized shipping container can be used as a substitute for an authorized courier on direct flights provided measures are taken to ensure that an appropriately cleared person will protect the container in the event the flight is diverted for any reason.

B. Material used for packaging must protect items and prevent them from breaking through their enclosures in transit. Bulky packages shall be sealed with tape laminated with asphalt and containing rayon fibers, nylon filament tape, or their equivalents.

21.2. TRANSMITTAL WITHIN DEPARTMENTAL FACILITIES

A. All NSI hand-carried between offices or operating units within a Department-owned or -leased facility shall be shielded to prevent inadvertent disclosure. The appropriate cover sheet shall be affixed to the top of the classified document (SF-703 for Top Secret, SF-704 for Secret, and SF-705 for Confidential). The cover sheet shall remain attached until the document is destroyed. A cover sheet that is not attached to any classified document is considered unclassified.

B. Individuals transmitting classified documents within a Department facility shall not carry classified documents into public areas (e.g., cafeterias, gymnasiums, etc.) while en route to their destination.

21.3. RECEIPT OF CLASSIFIED NATIONAL SECURITY INFORMATION

A document receipt, such as the Classified Material Receipt, Form CD-76, shall be completed for all transmissions of Top Secret and Secret information. A receipt for Confidential information is required only when transmitting Confidential information to a foreign government or its representative, or contractors.

21.4. METHODS OF TRANSMISSION

A. Top Secret Information. Before transmitting Top Secret information, the sender must coordinate its transmission with the Office of Security (OSY). Top Secret information shall be transmitted only by using one of the following methods:

1. Hand-carrying by an employee who has been granted a Top Secret security clearance and possesses a Courier Authorization Card, (CD-75) authorizing the employee to carry information up to Top Secret. The Security Contact must brief couriers on their responsibilities to protect Top Secret information.
2. The Defense Courier Service (DCS). The DCS must also be used for transmission of Sensitive Compartmented Information (SCI) and communications security (COMSEC) information.
3. Diplomatic pouch through the Department of State Diplomatic Courier System.
4. A cryptographic system authorized by the Director, National Security Agency (NSA), to process Top Secret information, or by a protected distribution system designed and installed to meet the standards included in the National COMSEC and Emanations Security (EMSEC) issuance system.

   Note: Top Secret information will not be transmitted through the U.S. Postal Service under any circumstances.

B. Secret Information. Secret information may be transmitted by one of the following methods:

1. Any of the means approved for the transmission of Top Secret information can be used to transmit Secret information. Secret information may be introduced into the DCS only when control of the information cannot remain in U.S. custody.
2. A designated employee or a contracted individual cleared at the Secret or Top Secret level, traveling on surface conveyance within a metropolitan area, may hand-carry the information provided the information is not transported across international borders and the courier maintains custody of the information at all times.

3. Secret information may be transmitted by United States (U.S.) Postal Service Express Mail and U.S. Postal Service Registered Mail within the U.S. and between the U.S. and its territories.
4. Secret information may be transmitted by U.S. Registered Mail through Military Postal Service facilities outside the U.S. and its territories provided that the information does not at any time pass out of the control of a U.S. citizen and does not pass through a foreign postal system or any foreign inspection.
5. Secret information may be transmitted by a cleared commercial carrier or cleared commercial messenger service as defined under the National Industrial Security Program. To ensure direct delivery to the addressee, the "Waiver of Signature and Indemnity" block on the U.S. Postal Service Express Mail, label 11-B, may not be executed under any circumstances. The use of external (street-side) express mail collection boxes is prohibited.
6. Secret information may be transmitted by a cleared and designated employee on scheduled commercial passenger aircraft within the U.S. and between the U.S. and its territories, subject to the procedures and restrictions set forth in paragraph 21.5, Hand-carrying NSI. The Servicing Security Office (SSO) or Security Contact must brief couriers on their responsibilities to protect NSI. The NSI must remain in the constant custody and protection of the courier at all times.

C. Confidential Information. Confidential information may be transmitted by using one of the following methods:

1. Any of the means approved for the transmission of Top Secret or Secret information and by the U.S. Postal Service Certified Mail within the U.S. and between the U.S. and its territories.
2. Confidential information can be transmitted by U.S. Postal Service First Class or Express Mail service provided the outer wrapping is stamped **"FIRST CLASS"** and **"POSTMASTER: DO NOT FORWARD. RETURN TO SENDER."** If a piece of Confidential mail weighs more than 12 ounces, it must also be marked **"PRIORITY MAIL."**
3. U.S. Postal Service Registered Mail (Return Receipt Requested) shall be used to send any of the following:
   a. NATO Confidential information
   b. Other Confidential mail addressed to Fleet Post Office (FPO) and Army Post Office (APO) addressees located outside the 50 states, District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories or possessions
   c. Confidential information to other addressees when it is uncertain whether their location is within U.S. boundaries

4. Confidential material may be sent to contractors and to agencies outside the Executive Branch by Certified or Registered Mail. The U.S. Postal Service Return Receipt shall be attached to the outside envelope.

D. NSI. Transmission of NSI over the telephone must be accomplished using Secure Telephone Equipment or other NSA-approved secure telecommunication equipment. NSI shall not be transmitted over any non-secure telephone, facsimile machine, or electronic mail system.

21.5. HAND-CARRYING NSI

A. **Restrictions.** Appropriately cleared personnel may be authorized to hand-carry NSI outside Department-controlled space subject to the following conditions:

1. The courier has an appropriate security clearance and has been issued a Courier Authorization Card, CD-75, as required in paragraph 21.7.
2. The classified material shall be hand-carried in a locked briefcase that serves as the outer enclosure.
3. The storage provisions of Chapter 33, Storage and Destruction Equipment, apply to all stops en route to the destination, unless the information is retained in the personal possession and constant surveillance of the individual at all times. The hand-carrying of NSI on trips that involve an overnight stopover is not permitted unless advance arrangements have been coordinated for proper overnight storage in a government facility or a cleared contractor's facility.
4. The NSI shall not be opened, read, studied, displayed, or used in any manner by the courier when traveling in public conveyances.
5. The courier shall not store NSI in any detachable storage compartment such as automobile trailers, luggage racks, aircraft travel pods, or drop tanks when traveling by private, public, or government conveyance.
6. The originating office must maintain a list of all NSI carried or escorted by traveling personnel.
7. Advance arrangements for appropriate overnight storage shall be made to ensure that the facility has authorized storage capability at the appropriate level. The storage capability should be available and accessible at the designated time of the visit. When traveling, the courier shall make contingent arrangements in the event that unforeseen problems occur that may result in late or delayed arrivals. The courier carrying NSI must understand his or her responsibility to safeguard the information while in transit and when arriving at their final destination.

B. **Hand-Carrying NSI Aboard Commercial Passenger Aircraft.** Appropriately cleared personnel may be authorized to hand-carry NSI aboard commercial passenger aircraft subject to the following conditions:

1. NSI may be hand-carried aboard commercial passenger aircraft only when there is neither time nor means available to properly transmit the information by other authorized means. The Director for Security (Director) shall grant permission to carry classified material overseas on a case-by-case basis. Requests for permission to carry NSI aboard a commercial passenger aircraft shall be submitted in writing to OSY by the SSO at least 10 working days prior to departure.
2. Prior to carrying NSI across international borders, the courier must make arrangements to ensure that the information will not be opened or viewed by customs, border, postal, or other inspectors, either U.S. or foreign.
3. The courier must travel aboard a U.S. carrier. Foreign carriers can be used only when no U.S. carrier is available. The courier must ensure that the information shall remain in his or her custody and control at all times.
4. The responsible Security Contact shall brief the courier concerning security safeguards and the need to possess departmental photographic identification. Written authorization from the Director is required by the courier to carry NSI aboard commercial aircraft. These items shall be displayed upon request by the appropriate airline personnel.
5. The NSI shall be sealed in double wrappings and carried in a briefcase or other carry-on luggage. The screening officials may check the envelope by using x-ray machine, flexing, touching, weighing, and so forth, but without opening the envelopes. Opening or reading classified documents is not permitted.

21.6. DESIGNATION OF COURIERS

The SSO may authorize an employee to hand-carry NSI up to the Top Secret level within the U.S. and its territories, except by commercial aircraft. This authorization is required for employees who routinely carry classified material to facilities in the same geographical areas. To be an authorized courier, the employee must hold an appropriate security clearance and possess a valid Courier Authorization Card, CD-75, as described in paragraph 21.7, Courier Authorization Card. Prior to obtaining NSI, the authorized courier must present a valid Courier Authorization Card to the holder of the NSI.

21.7. COURIER AUTHORIZATION CARD

A. **Courier Authorization.** The Department Courier Authorization Card, CD-75, authorizes the bearer to transport or hand-carry NSI on a recurring basis. The form will identify the holder by name, date of birth, and assigned operating unit. The card will include a date of issuance, expiration date, photograph of the holder, level of NSI authorized to be hand-carried, and the signatures of the holder and the SSO. A block is provided for the SSO's name and telephone number for clearance verification.

B. **Issuance and Control of the Courier Authorization Card.** Appropriately cleared personnel may obtain a Courier Authorization Card, CD-75, to hand-carry NSI outside Department-controlled space subject to the following conditions:

1. The SSO shall maintain accountability of all Courier Authorization Cards. Prior to receiving a Courier Authorization Card, the employee must have been granted a security clearance based on paragraph 20.1, Access to NSI.
2. The supervisor of the intended bearer shall request the issuance of a Courier Authorization Card in writing to the SSO. Upon verification of the employee's security clearance, the SSO will complete the Form CD-75 by affixing a current photograph of the employee, obtaining the necessary signatures, and laminating and issuing the Courier Authorization Card to the employee.
3. The bearer of the Courier Authorization Card must report the loss or damage of the card in writing to the SSO within five working days. The bearer may request a replacement card, which will be issued at the SSO's discretion. The loss of a Courier Authorization Card can result in forfeiture of courier privileges for an indefinite period of time, as determined by the SSO.
4. The Courier Authorization Card is valid for three years from the date of issue. The bearer must return the Courier Authorization Card to the issuing security officer upon termination of his or her security clearance, when the authorization is no longer needed, or when an occurrence dictates the need to withdraw the courier authorization, as determined by the issuing SSO.
5. The CD-75 does not authorize the courier to hand-carry NSI aboard commercial aircraft. Permission to hand-carry NSI aboard commercial aircraft shall be granted by the Director in accordance with paragraph 21.5.
6. The courier shall not use the Courier Authorization Card for purposes other than its intended use. Abusing or exceeding the authority of the card may result in disciplinary action.

Chapter 22. Custody and Accountability of Classified National Security Information

22.1. Custody of Classified National Security Information (NSI)

Any person who has possession of, or is charged with responsibility for NSI, must protect and account for that information. The following measures shall be applied to properly protect NSI:

A. While in use, NSI (e.g., documents, disks, etc.) shall be kept under continuous observation. NSI shall not be left unattended.

B. An office that receives NSI (in any form) and has no authorized storage equipment available must either return the NSI to the sender, arrange with another office to properly store the information, or destroy it by an approved method.

C. Under no circumstances shall NSI be left unattended, in an unauthorized storage container, or in the custody of a person who does not have the proper security clearance and an established need to know.

D. Custodians of NSI must ensure that persons who do not possess an appropriate security clearance and need to know, and are assigned to or visiting an office, do not take or read NSI, overhear classified conversations, or have visual access to NSI. NSI must not be placed or displayed in a manner where it can be seen through a window or a doorway.

E. NSI must be discussed only with those individuals who possess the appropriate security clearance and need to know. NSI shall not be discussed in public or other places where unauthorized persons could overhear it.

F. NSI must not be checked with baggage or left in a private residence, vehicles, hotel rooms and safes, aircrafts, train compartments, buses, public lockers, or other locations where the information could be compromised.

G. NSI should not be opened, read, studied, displayed, used, or discussed in any manner in a public conveyance or place. NSI must be appropriately stored in a General Services Administration (GSA)-approved security container at all times when not in use.

H. NSI must be covered with the appropriate level GSA Standard Form (SF) cover sheet (SF-703, SF-704, or SF-705).

22.2. Custody During Emergencies

A. In the event of fire, natural disaster, civil disturbance, or an evacuation of office space, NSI shall be protected by removing it under secure means, by placing it in safes, or by proper destruction. Persons who are away from their offices and have NSI in their possession at the time shall properly safeguard such information.

B. The head of each operating unit or Departmental office shall prepare a general plan for the emergency protection and destruction of NSI. The plan is vital in overseas locations and in locations where a potential threat to a Government facility exists. The plan shall

include all of the following:

1. The location and identity of the information to be destroyed
2. The priority for destruction, persons responsible for destruction, and the recommended place and method of destruction

C. The classified destruction plan shall be distributed to all cleared personnel working with NSI. The Security Contact shall ensure that personnel are briefed on the responsibilities of the plan.

22.3. RELOCATING CONTAINERS HOUSING NSI

When NSI is physically moved from one office or facility to another, it must be retained in a locked, approved security container. Supervisors or program managers responsible for control of the security container must notify the Servicing Security Office (SSO) prior to relocating a security container so the SSO can note the new location of the container. The custodian or other cleared personnel must maintain constant supervision of the container during the move. The SSO or Security Contact is responsible for notifying the Classified Control Point (CCP) of the new location of the container so this information is maintained in the Office of Security's (OSY) electronic database, Security Manager. The SSO or Security Contact must also annotate any changes to the relocation of the security container on SF-700, Security Container Information form. The SF-700 must be maintained in a container of equivalent or higher classification, preferably with the SSO.

22.4. ACCOUNTABILITY OF NSI

The following classified material must be properly controlled and accounted for by use of the OSY Security Manager database:

- All Top Secret
- Secret materials generated by Department of Commerce (Department) employees (original and derivative)
- Confidential materials generated by Department employees (original and derivative)
- North American Treaty Organization Secret
- All Secret document printed or downloaded from the Secret Internet Protocol Router Network (SIPRNet) in accordance with National Telecommunication and Information Administration (NTIA) SIPRNet Policy Letter #002

All Secret information not generated by Department employees shall be properly controlled and accounted for by use of written records or Security Manager. Confidential information shall be properly controlled and may be accounted for by use of written records or Security Manager.
To control and account for NSI using Security Manager each operating unit is encouraged to designate an office or unit CCP. The head of an operating unit may request an exception to this policy from the Director for Security.

Procedures shall ensure that the movement of NSI can be traced, dissemination is limited, prompt retrieval of information can be obtained, the loss of information can be detected, and excessive holdings and reproduction are limited.

22.5. ANNUAL INVENTORY AND DISPOSAL OF CLASSIFIED HOLDINGS

A. Offices maintaining NSI must conduct an annual inventory and review their classified holdings to reduce the amount necessary for operational and program purposes. All classified documents shall be reviewed upon initial receipt and during the annual inventory. The inventory shall include a review to determine possible downgrade, declassification, or destruction of classified holdings.

The Security Manager database shall be used to inventory and document all original and derivatively classified information and all Secret information printed from the Secret Internet Protocol Network (SIRPNet), as prescribed by this manual. At a minimum, internal tracking systems will perform all of the following functions:

- Describe the information, including the originator, classification level, subject, date of information, and number of copies
- Track internal routing
- Identify disposition by transmission outside the office or organization, by transfer to a storage area, or by destruction

B. On an annual basis OSY will print inventories from Security Manager. Custodians will validate the existence and or disposition of all document recorded in the system. Internal and hardcopy tracking systems will also be validated and confirmation of the entire inventory will be provided to OSY as instructed.

22.6. WORKING PAPERS

Working papers are drafts, notes, photographs, and so forth in paper or electronic form that are accumulated or created to assist in the formulation and preparation of a finished document. Working papers that contain NSI must be treated as follows:

- Dated when created
- Marked with the highest classification of the information that they contain
- Portion marked
- Protected in accordance with the highest classification
- Accounted for, controlled, and marked in the manner prescribed for a finished document of comparable classification when: (1) transmitted in any way; (2) permanently filed; or (3) retained for more than 180 days from the date of origin
- Destroyed when no longer needed

22.7. DESTRUCTION OF CLASSIFIED MATERIAL

A. **Authorized Destruction.** When no longer needed, classified documents shall be destroyed in a manner sufficient to preclude recognition or reconstruction of the NSI. The head of each operating unit, in consultation with the SSO, shall establish procedures for the proper destruction of NSI in the organization. Such procedures must ensure that adequate destruction records are maintained, authorized destruction methods are used, information is protected during transport, and the destruction is properly witnessed. Classified documents may be destroyed by one of the following methods.

1. **Shredding.** Only approved shredders shall be used for destruction of NSI. NSI must be shredded using a Department of Defense-approved high-security shredder. Shredders used for destroying classified material shall be properly marked with appropriate signage to identify its classified usage. The signage shall clearly identify the highest level of NSI that is authorized for destruction by the shredder. If uncertain, individuals should check with their Security Contact or SSO to verify the authorized level of the destruction equipment.

2. **Burning.** Classified documents shall be placed in burn bags marked as "Classified Waste Only." The destruction of Top Secret and Secret documents shall be witnessed and recorded in the electronic database or on the Commerce Department (CD) Form 481, Classified Document Control Record. A complete chain-of-custody shall be maintained from the moment classified materials are placed into a burn bag until the moment the burn bag contents are properly and completely destroyed. A classified material receipt shall be used to document the transfer of burn bags. Each person having access to the burn bags shall possess the necessary clearance. Documents shall be burned completely. Unburned residue cannot be allowed to remain or escape by wind or draft.

3. **Other Methods of Destruction.** Written approval shall be obtained from OSY before other methods of destruction such as melting, chemical decomposition, or mutilation are used to destroy classified material.

B. Storing and Transporting Material for Destruction. Classified material awaiting destruction shall be stored in an approved storage container. Individuals transporting classified waste material must provide adequate safeguards to prevent unauthorized disclosure of the information. Such waste must not be left unsecured or unattended when being transported to an authorized destruction site. The rules for transmission of NSI in Chapter 21, Transmission of Classified National Security Information, must be followed.

C. Records of Destruction. When classified documents are recorded in Security Manager, a record of destruction must also be recorded in Security Manager. Records of destruction shall include an unclassified description of the material, the date of actual destruction, name of the destroyer of the material, and the individual who witnessed the destruction. Destruction records shall be retained at least five years for Top Secret information and two years for Secret information. Holders of boxes or burn bags containing NSI marked for destruction must attach a classified material receipt when transferring the material to another individual for destruction. Each burn bag shall be clearly marked with all of the following identifying data:

1. Operating unit
2. Bag number
3. Name of person responsible for the contents of the burn bag

The following is an example of the transfer of three burn bags:

NTIA, bag 1 of 3, T. Jones
NTIA, bag 2 of 3, T. Jones
NTIA, bag 3 of 3, T. Jones

D. Classified Waste. Classified waste is defined as notes (working papers), NSI documents, disks, and other media containing NSI that is no longer needed. Binders, paperclips, cartridges, etc. must be removed before classified material to be destroyed is placed in burn bags as described in paragraph 22.7.A.

E. Destruction of Information Technology (IT) Material and Equipment. Guidance on the destruction of classified waste resulting from processing on IT systems, such as personal computers and printers, can be obtained from Office of the Chief Information Officer (OCIO).

22.8. END-OF-DAY SECURITY CHECK

A. The head of each operating unit or Departmental office, in consultation with the SSO, shall establish a system of security checks at the close of each working day to ensure that all of the following conditions are met:

1. All NSI has been returned to the appropriate GSA-approved security container and is properly stored.
2. All removable personal computer hard drives and working materials that contain NSI are properly stored in an appropriate GSA-approved security container.
3. Classified waste is properly stored or destroyed.
4. Wastebaskets and recycle containers do not contain classified material.
5. All security containers are double-checked to ensure they are locked.
6. All doors and windows to the area are locked.
7. Cryptographic cards are removed from security telephone equipment and properly safeguarded.
8. Alarms are properly activated.
9. The SF-702, Security Container Check Sheet, is completed in accordance with Paragraph 23.7 of this Manual.

B. The SF-701, Activity Security Checklist, shall be used to indicate that an end-of-day security check has been conducted each day that the office was occupied for duty purposes. The SF-701 shall be displayed and affixed to, or immediately adjacent to, the office exit door. The responsibility for the end-of-day security check shall be placed on the last employee to depart the office area. Individuals responsible for conducting the end-of-day security check must thoroughly check the entire work area where NSI is processed, handled, discussed, and stored, and then sign and date the SF-701.

Supervisors are responsible for establishing procedures in the office area to ensure these requirements are met. The originating office should retain each completed SF-701 for 90 days.

22.9. COPIER SECURITY

A. Introduction. This paragraph outlines the security precautions necessary to protect classified and other sensitive information from possible compromise as a result of copier use or other duplicating means. New technology available for copiers increases security vulnerabilities. The term copier refers to reprographics machines, facsimile machines, and printers that produce hard copy output, electronic blackboards that provide a reproduction of what is written on the board, and any machine with a combination of these functions.

B. Security Threats. Security measures shall address all of the following situations:

1. Individuals who may attempt to gain unauthorized copies of classified material.
2. The misuse of copiers by authorized persons.
3. The technical hazard of information retention through latent or residual images on machines or in electronic memory.

C. Designation of Copiers for Classified and Unclassified Reproduction.

1. Reproduction machines within the Department shall be designated as "approved" or "non-approved" for the reproduction of NSI, if they are located at a site that contains both classified and unclassified information. The SSO is designated to authorize copiers within his or her organization. Determination of approved copiers shall be based on the following:
   a. **Physical Location of the Copiers.** Approved machines shall be located in locked or secured areas to deny access to unauthorized users. If no locked or secure area is available, the copier shall be located away from high traffic areas where unauthorized persons are situated. The location shall allow continuous visual monitoring by office personnel of the copier during work hours.
   b. **Equipment Design.** All machines used for classified reproduction shall be approved for classified usage. These machines have few known security hazards and possess the most security design features (e.g., lock, key pad, and copy counter). It is recommended that copiers used for reproduction of NSI be equipped with removable hard drives. Machines designed with remote diagnostic capabilities shall not be used to reproduce classified material. Those machines that contain removable memory capabilities shall have the memory removed or degaussed by an authorized person prior to servicing by non-cleared personnel.
2. After designation of a copier as "approved" or "non-approved," it will be clearly identified as such by a posted notice. In addition, the SSO will issue classified reprographics equipment approval letters to the office managers possessing these machines. The letter will identify the machine(s) that are approved, the location, and the point-of-contact in the office. The point-of-contact will be required to coordinate with the SSO when potential security problems arise or when there are incidents of

possible compromise.

D. Approval. Reproduction of classified material shall be limited to those instances when it is absolutely necessary. Confidential and Secret information may be reproduced without prior approval of the originator unless otherwise indicated on the document. When Top Secret or Secret material is reproduced, the additional copies must be introduced into the written CD-481) or electronic accountability system (i.e., Security Manager). Reproduction of Top Secret material requires coordination with the originator and the Top Secret Control Officer.

E. Accountability/Control Logs. Records must be maintained to show the number and distribution of all reproduced Top Secret documents, special access documents, and those Secret or Confidential documents that bear special dissemination and reproduction limitations. Classified copier control logs are recommended but are not required for Confidential material. If used, these logs should record the identity of the individual making the copies, a description of the document(s), the originator, the number of copies made, and the date and time of reproduction. Reproductions of all Top Secret and Secret documents must be accounted for and controlled.

F. Copier Security Procedures. The following procedures shall be followed when reproducing NSI:

1. Cleared individuals will remain at the copier until classified reproduction is complete.
2. Digital copiers with electronic chip memory capabilities shall be used only in a stand-alone capacity. Digital copiers used to reproduce NSI shall not be connected to any network or telephone line.
3. Before leaving the copier, individuals must check the copier for any copies or originals that may be left in the copier.
4. Classified waste, such as rejected copies or blank copies run after classified material is processed, must be destroyed in accordance with Paragraph 22.7 of this Security Manual.
5. If the copier malfunctions and the copier cannot be cleared or the copies cannot be retrieved, the user or Security Contact shall notify the SSO to ensure that the copier is removed from approved service until the supervising office manager certifies that the malfunction has been properly cleared, at which time the copier may be re- certified for classified usage.

G. Scheduled Maintenance. The SSO or Security Contact shall be notified of the scheduled service visit and arrange for an appropriately cleared employee to be present. Any documents, image-retaining drum sheets, or memory chips removed from the machine shall be collected by the cleared employee and turned over to the SSO. No unescorted maintenance person shall be allowed access to any reproduction equipment used for the reproduction of classified materials.

22.10. MAIL PROCESSING FACILITIES

The supervisor of a mailroom shall develop procedures to protect NSI that may be contained in incoming mail, bulk shipments, or items delivered by messenger. Such procedures must limit access to NSI to appropriately cleared personnel only. U.S. Postal Service first class, certified, and registered mail should be presumed to contain NSI. Unless a mailroom has cleared personnel authorized to accept and open mail that may contain NSI, all incoming mail, bulk shipments, and items delivered by messenger must be forwarded directly to the individual addressed on the envelope. In addition, supervisors of mailrooms must establish measures to screen and/or x-ray incoming mail, bulk shipments, or items delivered by messenger. Mailroom supervisors should coordinate these measures with their SSO.

Chapter 23. Storage of Classified National Security Information

23.1. Protecting Classified National Security Information (NSI)

NSI must be stored in conditions that will provide adequate protection against access by unauthorized persons. Whenever NSI is not under the personal control and observation of a cleared person, it must be guarded by personnel with the appropriate security clearance or stored in a locked General Services Administration (GSA)-approved security container. The head of an operating unit or the Office of Security (OSY) may determine that more stringent requirements are needed based on the volume, nature, and sensitivity of the information to be protected in relation to other factors such as types of containers, presence of guards, vault-type space, or intrusion alarms.

23.2. Storage Standards

GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vaults, alarm systems, and associated security devices suitable for the storage and protection of NSI. OSY may establish additional supplementary controls to prevent unauthorized access. Safe-type filing cabinets conforming to federal specifications bear a test certification label on the locking drawer attesting to the security capabilities of the container and lock. On some early safes, this label was located on the wall inside the locking drawer. Safes manufactured after February 1962 will also be marked "GSA-Approved Security Container" on the outside of the top drawer. There are GSA-approved electronic combination locking devices for safes. To verify which devices are approved, contact the Servicing Security Office (SSO).

23.3. Storage of Top Secret Information

A. **Cabinets and Vaults.** When not in use, Top Secret information must be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type, changeable combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet minimum GSA standards. For more information, refer to Section IV if this Manual, Physical Security.

B. **Supplemental Controls.** Admittance to a Top Secret storage area shall be limited to authorized personnel. Persons not authorized access but whose presence in the area is temporarily required must be escorted and kept under constant observation. All NSI must be covered or otherwise protected from observation, disclosure, or removal. Top Secret information stored in a GSA-approved container shall also have supplemental controls as outlined in Paragraph 29.5.

23.4. Storage of Secret and Confidential Information

Secret and Confidential information shall be stored in a container, vault, or alarmed area that meets minimum GSA standards or one of the following exceptions to the standards:

A. **Secret and Confidential Information.** Secret and Confidential information shall be stored in a GSA-approved safe with a built-in, three-position, dial-type, changeable combination lock. Effective October 1, 2012 NSI cannot be stored in non-GSA-

approved security containers per 32 Code of Federal Regulations, Part 2001.43(b), Requirements for Physical Protection.

B. Bulky Secret and Confidential Information. Bulky Secret and Confidential information may be stored in vaults or other closed areas that have been approved and accredited for this purpose by the OSY, Counterespionage Division (CED). No area shall be used for classified open storage without prior accreditation and written approval by OSY CED or approval by the SSO in coordination with OSY CED.

23.5. CLASSIFIED COMBINATIONS

A. Protecting Classified Combinations. The combination of a lock used for the storage of NSI shall be afforded protection equal to that given to the highest level of NSI stored in the container. The combinations are classified and shall be recorded only on the Standard Form (SF) 700, Security Container Information form. The SF-700, Attachment 2, shall be stored in an appropriate level security container other than the container for which the combination is intended. Classified combinations that are recorded on anything other than the required SF-700, Attachment 2, are in violation of this policy. Security Contacts shall establish programs for the secure maintenance of combinations within their respective organizations and shall remind custodians and alternates that have access to security containers to memorize, record, and safeguard the classified combination at all times.

B. Changing Classified Combinations. Combinations to security containers shall be changed by the Security Contact, an appropriately cleared Government representative, a representative of OSY, or a bonded, appropriately cleared contractor of the Department of Commerce employed for this purpose. The requirement to change classified combinations on an annual basis no longer exists, except for containers holding North Atlantic Treaty Organization information. Combinations shall be changed in any of the following situations:

1. When a container is placed in use.
2. When an individual knowing the combination no longer requires access to the container.
3. When the combination is subject to possible compromise.
4. When a container is taken out of service. Built-in combination locks shall be reset to the standard combination 50–25–50 (10–20–30 for padlocks) prior to removal from office space.

C. Security Container Information. Each Security Contact shall maintain a record of each vault, secure room, or container used for storing NSI. This record shall identify the current location of the container or room, and the name, home address, and home telephone number of each individual (custodian and/or alternate) responsible for, and having access to, the combination. The SF-700 must be used for this purpose. Instructions for completing the form are printed on the form itself. All security

equipment, including security containers used for the storage of NSI, shall be controlled by the Security Manager system. The Security Contact of each operating unit shall be responsible for ensuring that the Classified Control Point (CCP) maintains a record of pertinent container information.

D. **Maintaining Classified Combination Records.** The operating unit shall forward Attachment 2 of the SF-700 to the Security Contact or OSY, for safeguarding. When completed, Attachment 2 of the SF-700 is classified and therefore must be transmitted in accordance with Chapter 21 of this Manual. Attachment 2 is the sealed envelope portion of the SF-700 that holds the classified combination. The Security Contact may choose to secure this form in his or her GSA-approved security container or forward the form to OSY for safeguarding. Custodians or alternates shall not store Attachment 2 of their SF-700 form in their security container. SF-700 forms shall be kept current at all times in accordance with Paragraph 23.5.B. Classified container combinations are classified and must be treated as such when transmitted from one person/location to another.

E. **Access to Classified Combinations.** Only appropriately cleared and authorized employees shall have access to classified combinations. The number of employees with access shall be kept to a minimum (normally two to three) and be clearly identified on the SF-700. Combinations shall not be provided to anyone who is not identified on the SF-700. The custodian or alternate is responsible for properly safeguarding the classified combination and preventing unauthorized access to the security container.

23.6. OPEN-CLOSED SIGNS

Reversible OPEN–CLOSED signs, or similar signs, should be used as reminders on all classified storage containers each time they are locked or unlocked.

23.7. SECURITY CONTAINER CHECK SHEET

An SF-702, Security Container Check Sheet, shall be placed on the exterior of each classified security container to record each time the container is opened, closed, and double-checked. The individual conducting such actions shall include his or her initials in the applicable part of the form. Each opening and closing shall be recorded using the individual's initials and the time of the opening and the closing. The "Checked By" column will be used every day that the office is occupied to conduct work. This is done to ensure that an individual who failed to complete the "Opened By" and "Closed By" blocks did not leave the security container open accidentally. The "Guard Check" column is optional. The individual who conducts the end-of-the-day double-check of the container must ensure that the container is properly locked and secured by pulling on the handles of the drawers and then spinning the combination dial at least four rotations. Although it is not always possible, the person conducting the end-of-the-day double-check of the security containers should not be the same person who opened and closed the security container during the duty day. This procedure provides an additional security measure to ensure that NSI in the office is protected. Supervisors are responsible for establishing procedures to ensure that the requirements in this paragraph are met.

23.8. SURPLUS SECURITY CONTAINERS

Security containers no longer used for the storage of NSI may be transferred to other areas where they are needed or sent to surplus. Prior to moving any container, the container shall be thoroughly searched for classified material. All NSI shall be removed. Areas to be searched include: between, behind, and underneath the container and behind, under, and on the sides of all drawers. This search may involve removing each drawer for thorough inspection (because materials may have inadvertently fallen behind the drawer and are not visible without removing or lifting the drawer). The Security Contact must declare the container empty by placing a written statement on the outside front of the container indicating the date of the inspection, the person who conducted the inspection, and the unit and office that last used the container. In addition, prior to moving any security container with a built-in combination dial, the combination shall be reset to the standard combination of 50–25–50. The written statement on the outside of the container shall state that the combination has been reset. The Security Contact must remove and destroy Attachment 1 of the SF-700 located inside the control drawer. No security container shall be relocated or taken out of service without first notifying the SSO or Security Contact, who must ensure the action is annotated in the management information tracking system and reflected on the SF-700. If the combination cannot be changed because of a mechanical problem with the dial, the existing combination shall be annotated on the written statement.

Chapter 24. Security Compromises, Violations, and Sanctions

24.1. PROTECTING CLASSIFIED INFORMATION

A. The compromise of classified information presents a threat to national security. Once a compromise has occurred, the damage to the national security interests of the United States must be determined and appropriate measures taken to negate or minimize the adverse effect of the compromise. Whenever possible, action shall be taken to regain custody of the documents or materials that were compromised. In all cases, however, appropriate action must be taken to identify the source of the compromise, determine the reason for the compromise, and identify any corrective action taken, or take any corrective action necessary to ensure further compromise of classified information does not occur.

B. Each employee or individual who has access to classified information is responsible for complying with the guidance in the Implementing Directive for Executive Order (E.O.) 13526, Classified National Security Information, and this Security Manual concerning protection of such information. Any appropriately cleared person with an established need to know, having access to and/or possession of classified information is responsible for all of the following:

1. Protecting classified information from unauthorized persons, including properly securing the information in approved security containers or facilities whenever it is not under the direct control or supervision of authorized persons.
2. Meeting accountability and control requirements as prescribed in this Security Manual and other guidance issued by the Office of Security (OSY).
3. Disposing of classified material by an approved method when the materials are no longer required, not necessary to the program, or can be declassified in accordance with the E.O. 13526.
4. Reporting the loss or possible compromise of classified information immediately to the operating unit's Security Contact and OSY, Counterespionage Division (CED).

C. Any known or suspected mishandling, loss, unauthorized disclosure, or possible compromise of classified information warrants a preliminary inquiry and/or investigation. Inquiries and investigations into potential security violations shall be immediate and thorough in order to determine all facts surrounding the incident, possible impact or damage to national security, determination of whether a possible pattern of violations exists, and other relevant information pertaining to the violation. The inquiry and/or investigation shall identify what actions were taken to prevent any future violations (see paragraph 24.10, Report of Security Violation, below).

24.2. APPLICABLE DEFINITIONS

A. Security Infraction. A security infraction occurs when classified information is not properly safeguarded in accordance with appropriate E.O.s, federal regulations, and this

Security Manual but does not result in the actual or probable compromise of the material.

B. Security Violation. A security violation occurs when classified information is not properly safeguarded in accordance with appropriate E.O.s, federal regulations, and this Security Manual and results in the actual or probable compromise of classified information, or when a possible compromise cannot be ruled out.

C. Compromise. An actual or probable compromise of classified information constitutes a threat to the national security. A compromise of classified information occurs whether the act was intentional or unintentional.

1. A probable compromise occurs in one of two circumstances:
   a. Classified material is recovered outside of a controlled area.
   b. The controlled area or facility is unattended and not properly secured.
2. An actual compromise occurs when classified information has been released or disclosed to an unauthorized person and the damage to national security is deemed likely or determined to have occurred as the result of this unauthorized disclosure.

D. Controlled Area. A controlled area is a specifically designated area - where classified information has been authorized for handling, storage, discussion, or processing, and where supplemental controls have been established in accordance with applicable regulations.

24.3. COMPROMISE OF CLASSIFIED INFORMATION

A. Compromise of classified information presents a threat to national security and can result from espionage; mishandling of classified information; illegal technology transfer; publication of books and treaties; public release of articles, videos, or press releases; or displays at trade shows, conferences, or symposia. Compromise can occur through the loss of classified information or equipment. Once a compromise has occurred, the damage to U.S. interests must be assessed. Immediate remedial action must be taken to ensure that further compromise does not occur. This may include suspension of the violator's access to classified information pending a completed investigation.

B. Any employee who has knowledge of an actual or possible compromise or who discovers that classified information (in any form) is missing must report the loss or possible compromise to the appropriate Security Contact/Servicing Sercurity Officer (SSO) or OSY/CED, immediately following the discovery. The Security Contact/SSO must verbally report the discovery of a security compromise to OSY/CED. In the case of a known or suspected compromise involving Top Secret or special access information, the compromise shall be reported immediately to the Director for Security (Director).

C. When there has been a compromise of classified information originated by an office or employee of the Department, a damage assessment must be initiated by the Director. The Director shall make this information available to the appropriate authorities for further action as necessary.

D. A case of espionage and/or deliberate compromise of classified information must be reported to the Director. The Director will coordinate further investigative actions with OSY/CED, Investigations and Intelligence Division, the Office of the Inspector General, and/or other appropriate federal investigative agencies required to conduct an Espionage Damage Assessment.

24.4. VIOLATIONS SUBJECT TO ADMINISTRATIVE SANCTIONS

A. Departmental employees and contractors may be subject to administrative sanctions if they knowingly, willfully, or negligently do any of the following:

1. Disclose to unauthorized persons information properly classified under E.O. 13526, or prior orders.
2. Classify or continue to classify information in violation of E.O. 13526, and its implementing directives.
3. Create or continue a special access program contrary to the requirements of E.O. 13526.
4. Violate any other provision of E.O. 13526, or its implementing directives.

B. The Department's Information Technology Security Officer (ITSO) and the operating unit's ITSO shall report any violation involving the improper processing of classified information on automated systems to OSY. Because the Director for Security is the senior agency official designated by the Secretary of Commerce to direct and administer the Department's program under which National Security Information (NSI) is classified, safeguarded, and declassified, the Director shall review all IT security violation reports involving classified information. In addition to the reporting requirement, any person aware of improper processing of classified information on automated systems by another person shall report the violation directly to his or her Security Contact or SSO, who in turn, shall immediately notify the appropriate ITSO.

C. National defense information properly classified pursuant to E.O. 13526, or other applicable E.O.s is expressly exempt from public disclosure under 5 U.S.C. 552 (b) (1).

24.5. ADMINISTRATIVE SANCTIONS FOR SECURITY VIOLATIONS

A. If a security violation or compromise has been investigated and confirmed, disciplinary action may be taken against the person(s) responsible for the offense.

1. Administrative sanctions for security violations or compromise of classified information may include, but are not limited to, oral or written reprimand, suspension without pay, revocation of access to NSI, or removal from the position or service in accordance with applicable law and DOC regulations.

2. For security violations of a serious, willful, or grossly negligent nature, an individual's continued eligibility for access to classified information shall be evaluated by the Assistant Director, CED, who shall make a determination concerning the employee's continued access to NSI. If circumstances warrant, the

employee's operating unit may also take disciplinary action under the provisions of applicable laws and regulations.

3. When OSY determines that an individual is responsible for a security infraction a determination must be made regarding the person's continued access to classified information. In these instances, the official conducting the inquiry must ensure the incident is reported accurately and all pertinent information is included in the report.

4. -OSY may refer such cases to the Office of the Inspector General or other appropriate federal investigative agencies for follow-up action as necessary.

B. If an individual occupying an Original Classification Authority (OCA) position commits any of the violations noted in paragraph 24.4, sanctions may also include termination of OCA and loss of eligibility for access to NSI. If an OCA official demonstrates reckless disregard or a pattern of error in applying the classification standards of E.O. 13526, the Director may promptly remove the individual's authority to make original classification decisions.

C. If the security violation does not warrant reprimand, suspension, or loss of eligibility for access to NSI, sanctions may include other administrative actions, such as refresher training, implementation of different methods or procedures to prevent a similar incident from occurring, and/or an element included in the employee's performance plan. If an element already exists in the performance plan, it should be evaluated annually.

1. When an employee has committed a security infraction within a 12-month period, a letter shall be sent by the SSO to the employee and his or her immediate supervisor directing the employee to be more conscious of proper security practices. The employee will be directed to contact his or her SSO to promptly schedule and attend a NSI Refresher Briefing.

2. If an individual has committed a second security infraction within a 12-month period and the SSO deems the infractions to be sufficiently serious, the Security Officer may recommend appropriate disciplinary action to OSY, citing the infractions as an indicator of a more serious problem. OSY will confer with the appropriate operating unit and Servicing Human Resources Office concerning recommendations for disciplinary action based on multiple security infractions.

D. Whenever an action is being considered against an employee responsible for the compromise of classified information, the investigative report, damage assessment, and recommendations for administrative sanctions shall be forwarded to the employee's operating unit head, Office of Human Resources Management, and Office of General Counsel for action.

24.6. CRIMINAL SANCTIONS

A. The release or disclosure of classified information to unauthorized sources may result in the imposition of criminal sanctions, including fines and/or imprisonment, in accordance with 18 U.S.C. § 641, 793, 794, 798, 952, and 1924, and 50 U.S.C. 783(b).

B. If at any time during the administrative inquiry or investigation into an alleged security violation it is suspected that a criminal statute may have been violated, the inquiry and/or investigation shall be stopped immediately. The investigator should notify the Director for coordination of the criminal aspects of the investigation with the Office of the Inspector General and/or other appropriate federal investigative agencies. Disciplinary action may be withheld until it is determined that criminal charges will be pursued, however, this must be determined on a case by case basis.

24.7. RECORDS OF SECURITY VIOLATION AND PERFORMANCE RATING

E.O. 13526, Classified Nationa Security Information, directs that the management of classified information shall be a critical element in the performance plan of original classifying authorities, security managers and specialists, and all other personnel granted access to classified information.- Heads of operating units are responsible for implementing this provision of the E.O. within their respective organizations.

24.8. REPORTING SECURITY VIOLATIONS

A. Any person who has knowledge or suspects the loss or possible compromise of classified information (in any form) or any person who discovers classified information out of the proper control shall take both of the following steps:

1. If applicable, take immediate custody of such information and safeguard it in an appropriate manner. This responsibility includes protecting classified information that is discovered improperly safeguarded or unsecured.
2. Immediately report the loss or possible compromise of classified information to the Security Contact or SSO. In some cases, initial notification of loss or possible compromise may be reported directly to OSY headquarters.

B. Individuals who report the loss or possible compromise of classified information may be asked to submit a signed statement, and in rare cases, to make a sworn declaration. Employees are required to cooperate in all administrative investigations, to report all information of which they have knowledge, and to give complete and truthful answers. Failure to do so may result in disciplinary action.

C. When a Security Contact receives either a verbal or a written notice of a security violation, he or she must immediately notify the SSO of the discovery. Based on the information obtained in paragraph 24.8.A above, the SSO shall immediately conduct an inquiry to determine whether a security infraction or violation has occurred and identify the individual responsible for the infraction or violation. A copy of the completed inquiry will be forwarded to OSY in Washington, D.C., within five working days.

D. OSY shall evaluate the inquiry and determine whether a further investigation of the incident is necessary. If an investigation is conducted and a damage assessment determines that classified NSI has been compromised, the Director will recommend appropriate measures to minimize the damage to the national security, prevent further compromise, and review security procedures and practices in the offices involved in the

compromise. The Director may also recommend disciplinary action to the head of the operating unit as appropriate. Such action will be done in consultation with the Office of Human Resource Management.

E. All apparent security violations shall be made a matter of record pending final adjudication. If OSY determines that the alleged security violation is not valid, the documentation relating to the reported incident shall be destroyed 90 days after the date of the adjudication. If the alleged security violation is determined to be valid, a written notification of this determination will be provided to the individual responsible for the security violation. The SSO shall retain a copy of all documentation relating to the security violation for 12 months from the date of the report. The individual responsible for the security violation will be notified in writing and advised of the possible consequences of this violation or subsequent violations or infractions.

F. At the end of the fiscal year, each SSO shall forward to OSY a summary of security violations and infractions that occurred in his or her respective organizations during the preceding fiscal year (see paragraph 16.6, Reporting Requirements). The summary shall include a list of violations and infractions by name, operating unit and office, description or nature of the incident, impact on national security that resulted from any violation, and any corrective or disciplinary action taken. Negative responses are required.

G. The Director shall report any violations of law, including an action resulting in unauthorized disclosure of classified information, and any evidence reflected in classified information that reveals possible violations of law to the Office of the Inspector General. The Director shall also report any knowing and willful security violations described in E.O. 13526, to the Director, Information Security Oversight Office (ISOO).

24.9. PRELIMINARY SECURITY INQUIRIES

A. Based on a verbal or written report from an employee or an operating unit Security Contact of a possible security violation, the SSO or his or her designee shall conduct an inquiry to determine whether a security infraction or a violation has occurred, the source and reason for the security infraction or violation, the appropriate measures or actions to minimize or negate the adverse effect of the security incident, and the seriousness of damage to national security interests. The SSO shall ensure that all security inquiries or investigations are completed within the period specified by OSY, with sufficient information to determine the validity of the alleged violation. The SSO shall use the (Memorandum), Report of Security Violation, to report all security infractions or violations. A copy of the completed report will be forwarded to OSY headquarters in Washington, D.C.

B. The official conducting the inquiry shall be appropriately cleared and shall conduct the inquiry in a fair and unprejudiced manner. The Report of Security Violation shall be provided as the written report to the SSO. Security inquiries will include all of the following:

1. A brief, unclassified description of the subject material possibly compromised, including the subject and date of the information, originator, classification level, and type of material (e.g., cable, memorandum, disk, notebook, or classified discussion).
2. A detailed narrative statement providing the circumstances of the possible compromise, the identity of the person(s) who had or may have had access to the information, and a determination of whether a compromise in fact occurred.
3. The dissemination of the material with the date and time the material was initially received by the office reporting the inquiry, and if applicable, the circumstances under which the loss was realized and the steps taken to relocate or protect the material.
4. The identity of the person or procedure responsible for the loss and the action(s) taken to prevent a recurrence of the loss.

C. The SSO shall ensure that all security inquiries or investigations are completed within the time period specified by OSY, with sufficient information to determine the validity of the alleged violation.

24.10. REPORT OF SECURITY VIOLATION

A. Security Contacts or SSOs who receive notice of an apparent security violation will provide a written Report of Security Violation and conduct a preliminary inquiry to determine whether the incident constitutes a valid security violation. The Report of Security Violation will be forwarded to OSY for evaluation to determine whether the violation has resulted in a security compromise that requires additional investigation and/or follow-up action. The report shall not be classified or administratively controlled in and of itself. If the security violation itself is classified, then a separate, classified page should be attached to the Report of Security Violation. If classified or administratively controlled attachments accompany the report, the form shall be appropriately marked to be declassified or decontrolled upon removal of the attachments.

B. The individual conducting the preliminary inquiry will provide a brief description of the circumstances of the security violation and the level of classification in the Report of Security Violation. Other information to be provided by the investigator includes the nature of the violation, the date and time of the report, the location of the incident, and the regulation referenced for the violation. The preliminary inquiry will then be provided or forwarded to the SSO for review.

C. The SSO will review the preliminary inquiry and complete the Report of Security Violation, indicating the corrective action taken to secure the information and/or ensure that future loss or disclosure does not occur. The SSO will also determine the time period during which the classified information was not protected, the name of the person(s) responsible for the alleged violation, and the identity of individuals possibly having access to the unsecured information.

D. Upon completion of the preliminary report, the Report of Security Violation and any related information describing the incident shall be forwarded to the individual allegedly responsible for the security violation. This individual shall describe his or her actions in the report and identify the circumstances surrounding the alleged security violation.

E. The SSO shall review the Report of Security Violation and provide an assessment concerning the damage, potential damage, or compromise to NSI.

1. If the SSO determines that classified information has not been compromised but that established security procedures have not been met, the SSO may issue a written notice of security violation to the individual's immediate supervisor and recommend the individual responsible for the violation receive an NSI refresher briefing. The original Report of Security Violation shall remain on file with the SSO for one year unless similar violations occur within that period. If a similar security violation occurs within the one-year period, the SSO shall forward the reports to OSY headquarters in Washington, D.C., for inclusion in the individual's official Personnel Security file. All reports will remain in the individual's Personnel Security file indefinitely.
2. If the SSO determines that there has been a probable or actual compromise of classified information, he or she shall issue a written notice of security violation to the individual's immediate supervisor and forward the completed Report of Security Violation to OSY headquarters. OSY will review the report to determine whether any of the following is true:
   a. An actual violation occurred.
   b. There is a probability of a compromise of NSI.
   c. The violation resulted in a risk to national security or damage to the Department's mission and responsibilities.
   d. Further investigation of the incident is warranted (investigative assistance may be sought from other agencies, if necessary).

24.11. SECURITY INVESTIGATIONS

A. When a compromise of NSI occurs or there is a probability of damage to the national security adversely affecting the Department's mission, OSY shall initiate an investigation, coordinate with appropriate authorities to conduct an investigation, or direct the SSO to conduct the investigation.

B. The investigation shall include a copy of the Report of Security Violation and supporting statements from any employees involved (see paragraph 24.10.A above).

C. OSY shall notify the originator of the information that a loss or possible compromise has occurred so that a damage assessment can be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The originator of the classified information shall conduct a damage assessment as prescribed in paragraph 24.12 below.

1. Whenever a compromise involves the classified information or interests of an agency outside the Department, OSY and other agencies shall be notified and shall advise other agencies of the circumstances and findings that affect their information or interests. Whenever a damage assessment requires the coordination of two or more agencies, the affected agencies shall agree upon the assignment of responsibility for the assessment.
2. Whenever a compromise occurs within an agency that is not responsible for the damage assessment, the agency shall provide all data pertinent to the compromise to the agency responsible for conducting the assessment.

D. OSY shall maintain a record of any disclosed classified information that was evaluated and investigated under the auspices of a Servicing Security Office. Based on the conclusions of the investigation, OSY may recommend that appropriate disciplinary action be taken against the person(s) responsible for the incident.

E. Disciplinary action for security violations is administered by an employee's immediate supervisor in consultation with the servicing Human Resources Office. As the senior agency official responsible for security matters, however, the Director may review the recommended disciplinary action to determine whether the action taken is sufficient or adequate for the violation committed. The Director may recommend additional administrative actions, such as refresher security training or implementing different methods or procedures to prevent a similar incident from occurring.

F. A damage assessment shall be conducted when there is a reasonable expectation of damage to national security. The content of the investigation report establishes a need to conduct a damage assessment. The operating unit head shall be consulted regarding impact or damage to the program information resulting from the security violation or compromise.

24.12. DAMAGE ASSESSMENT

A. When a security compromise has been discovered or determined, OSY will request the originator to conduct a damage assessment to obtain all of the following information:

1. Identification of the source, date, and circumstances of the compromise.
2. Classification of the specific information lost.
3. An unclassified description of the specific information.
4. An analysis and statement of the known or probable damage to the national security that has resulted or may result.
5. An assessment of whether existing countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.
6. An assessment of other appropriate corrective, administrative, disciplinary, or legal actions to be taken in an organization or against an individual.

B. The assessment must determine how the compromised information should be handled. Options include the following:

1. Remain at the same classification level.
2. Be modified to minimize or nullify the effects of the compromise.
3. Be downgraded, declassified, or upgraded.

C. Holders of any classified information must be informed of any changes to the classification of compromised information.

24.13. SECURITY VIOLATIONS INVOLVING OTHER AGENCIES

A. Whenever a compromise involves the classified information or interests of more than one agency, each agency or organization undertaking a damage assessment shall advise the other agencies of the circumstances and findings that affect their interests.

B. Whenever a compromise of the U.S. classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals employed by international organizations, the agency performing the damage assessment shall ensure, through appropriate intergovernmental liaison channels, that all information pertinent to the assessment is obtained. Whenever more than one agency is responsible for the assessment, the agencies shall coordinate the request prior to transmittal through appropriate channels.

C. The Director of Central Intelligence or other appropriate official shall be consulted immediately whenever a possible compromise of Sensitive Compartmented Information (SCI) has occurred.

D. Whenever a possible compromise exists involving North Atlantic Treaty Organization (NATO) information, coordination with the Central U.S. Registry is required.

Chapter 25. Safeguarding North Atlantic Treaty Organization Information

25.1. PURPOSE

The purpose of this chapter is to establish and issue the guidance, criteria, and procedures required to ensure Department of Commerce (DOC) compliance with the implementation of United States Security Authority for North Atlantic Treaty Organization (NATO) Affairs (USSAN) Instruction 1-07, "Implementation of North Atlantic Treaty Organization Security Requirements."

25.2. NATO CLASSIFIED INFORMATION

A. USSAN provides for U.S. implementation of NATO Security Procedures. When NATO or COSMIC precedes a classification, the material is the property of NATO, but the information remains the property of the originator. For further instruction, check with the Office of Security (OSY) and see USSAN Instruction 1-07, 3.3, "*Requirements for Access to NATO Classified Information*," and 3.5, "*Access by Non-NATO Nationals.*" The determination of whether or not a U.S. document is to be released to NATO-member countries is the responsibility of the originator in compliance with the U.S. need-to-know principle. Classified information released to NATO remains the property of the originator and may not be given to any non-NATO nation or to any other international organization except by the originator.

B. NATO has four levels of classified information: Cosmic Top Secret (CTS), NATO Secret (NS), NATO Confidential (NC), and NATO Restricted (NR), which are defined as follows:

1. **Cosmic Top** Secret. This security classification applies to information whose unauthorized disclosure would result in, or could reasonably be expected to result in, exceptionally grave damage to NATO. The marking COSMIC is applied only to Top Secret documents prepared for circulation within NATO. Cosmic is a marking that, when applied to a document, signifies that both of the following conditions apply:
   a. The document is the property of NATO and may not be passed outside the organization except by the originator or with the OSY's consent; and
   b. The document is subject to the special security protection outlined in USSAN Instruction 1-07.
2. NATO Secret (NS). This security classification applies to information whose unauthorized disclosure could reasonably be expected to cause grave damage to NATO. NATO Secret is a designation that, when applied to a document, signifies that both of the following conditions apply:
   a. The document is the property of NATO and, if bearing a security classification, may not be passed outside the organization except under conditions outlined in USSAN Instruction 1-07, 3.5, "Access by Non-NATO Nationals."

b. The document, if bearing a security classification, is subject to the security protection outlined in USSAN Instruction 1-07.

3. **NATO Confidential**. This security classification denotes information whose unauthorized disclosure could reasonably be expected to cause damage to NATO.
4. **NATO Restricted (NR).** This security classification applies to information whose unauthorized disclosure would be prejudicial to the interests or effectiveness of NATO. The United States does not have a security classification equivalent to NR; therefore, documents marked NATO Restricted will be protected in accordance with the requirements of "FOUO" (For Official Use Only) information. Documents originated by NATO that are marked NR shall be marked with the following additional notation: "To be safeguarded in accordance with United States Security Authority for NATO (USSAN) Instruction 1-07." Additional detailed requirements for the protection of NR are contained in the NATO document, AC/35-D/1034, "Supporting Document on the Security Protection of NATO RESTRICTED Information."

C. The USSAN Instruction 1-07, "*Implementation of North Atlantic Treaty Organization Security Requirements*," is issued for compliance throughout the civilian and military elements of the Department of Defense (DoD) and all federal departments and agencies handling NATO-classified material and information. The OSY maintains a copy of this instruction.

25.3. OTHER NATO INFORMATION

A. NATO Unclassified (NU). This marking is applied to NATO information that does not require security protection. NATO Unclassified information may be handled as U.S. Unclassified information. NU shall only be used for official purpose. NU information may also carry administrative or dissemination limitation markings. The basic principles and minimum standards for handling NU information are contained in the NATO document, C-M(2002)60, "*The Management of Non-Classified Information.*"

B. ATOMAL. This marking is applied to either U.S. Restricted Data (RD) or Formerly Restricted Data (FRD) or United Kingdom Atomic information that has been officially released to NATO. Atomal information is classified Cosmic Top Secret Atomal (CTSA), NATO Secret Atomal (NSA), or NATO Confidential Atomal (NCA), depending on the damage that would result from unauthorized disclosure. Security provisions for ATOMAL information are contained in C-M(64)39, "*Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding Atomic Information*," and in C-M(68)41 (6th Revision), "*Administrative Arrangements to Implement the Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding ATOMAL Information.*" U.S. personnel are directed to consult these documents directly and adhere to their provisions.

25.4. COMMERCE NATO SUB-REGISTRY

A. All NATO documents forwarded to the DOC are received by the sub-registry located in the DOC headquarters in Washington, D.C. The sub-registry is the primary point of contact (POC) for accountability and control of all NATO documents received by the Department. For further directions, please see USSAN Instruction 1-07, 5.4, "*The Registry System.*"

B. The Department has several approved control points for accountability, control, and storage of NATO material. The Servicing Security Officer or the OSY should be contacted to obtain a list of the Departmental control points.

25.5. SECURITY CLEARANCE REQUIREMENTS FOR NATO

A. Access.

1. Access to NATO classified information requires a final U.S. security clearance at the equivalent classification level (i.e., access to NATO Cosmic Top Secret requires a U.S. Top Secret security clearance and access to NATO Secret information requires a U.S. Secret security clearance). Access to NATO classified information must be limited to the minimum number of personnel who require such access to perform their assigned duties. The OSY maintains a list of all DOC personnel cleared for NATO access. Each NATO Control Point shall maintain a roster of personnel cleared for NATO access. Verification of NATO access shall be obtained from the Servicing Security Officer or in the OSY.
2. Although NATO Unclassified information does not require security protection, it may only be released to non-NATO nations, organizations, and individuals when such release would not be against the interest of the NATO. Any procedures considered necessary for such release will be decided independently by member nations and NATO commands and agencies.

B. Temporary Access.

1. In wartime or in periods of mounting international tension when emergency measures are required, the OSY may, in exceptional circumstances, grant temporary NATO access to personnel who do not possess the requisite security clearance, provided that such authorization is absolutely necessary, and there are no reasonable doubts regarding the trustworthiness of the person concerned. Requests for such emergency access must be fully justified and documented.
2. Whenever such emergency access is granted, a record of the authorization will be made by the OSY, which will, as soon as possible, institute the procedures necessary to fulfill the normal clearance requirements.

25.6. NATO BRIEFING AND DEBRIEFING

A. Before access to information classified NATO Confidential and above is granted, U.S. personnel must receive a NATO security briefing. The OSY shall conduct all NATO

security briefings and maintain copies of all security briefing certificates for a minimum of two years from the date of such briefing.

B. Uncleared personnel may be authorized access to NATO Restricted information when it is determined there is a need for such access in the performance of official duties. A personnel security clearance for such access is not required, but each person must receive a NATO security briefing.

C. A NATO security briefing shall be provided to each person who is exposed to frequent contact with representatives of countries with special security risks. A list of "countries with special security risks" is provided in USSAN Instruction 1-07, 3.5.3.1. This list is maintained in the OSY, Counterespionage Division (CED).

D. Persons who have access to NATO classified information and who intend to travel to or through (including scheduled stopovers by air travel) countries with special security risks, or to any destination by any form of transport that belongs to, is registered in, or managed from such a country, shall be given a thorough briefing about the security hazards of that country or geographical area before they travel. During the briefing, they will be instructed to report immediately on any occurrence that could have security implications, no matter how unimportant it may seem.

E. When access to classified NATO information is no longer required, personnel will be debriefed. All debriefings must be recorded and shall be maintained by the OSY for a minimum of two years from the date of debriefing.

25.7. STORAGE, TRANSFER, AND DESTRUCTION OF NATO DOCUMENTS

A. Storage.

1. **NATO Classified Documents**. NATO classified documents shall be stored as prescribed in USSAN Instruction 1-07. NATO documents shall not be commingled with U.S. or other documents. NATO documents may be filed in the same drawer as other non-NATO documents if they are segregated and clearly identified as NATO files. All personnel who have access to a security container used for the storage of NATO classified information must be cleared at the appropriate level and briefed for NATO access.

2. **NATO Restricted Documents.** NATO Restricted documents (unclassified material) may be stored as prescribed in USSAN Instruction 1-07. NATO Restricted documents are unclassified but are protected from public access and release as "FOUO" (For Official Use Only) or "SBU" (Sensitive But Unclassified) material.

3. **COSMIC Top Secret Documents.** The DOC does not have the authority to store COSMIC Top Secret documents.

4. **Container Combinations.** The combinations of authorized security containers containing NATO classified documents shall be changed annually in accordance with USSAN Instruction 1-07.

5. **Inventory**. NATO material classified Secret and above shall be accounted for and inventoried every six months. NS sub-registries shall be inspected for compliance with security procedures by the Central U.S. Registry (CUSR) at least every 24 months or at a frequency to be determined on a case-by-case basis by the Chief, CUSR. Sub-registry self-inspection reports will be forwarded to the CUSR, with a copy retained by the sub-registry, until the next inspection by the CUSR. Sub-registries shall inspect control points and shall retain a copy of the inspection report on file.

B. Packaging and Transmission of NATO Documents.

1. Cosmic Top Secret, NATO Secret, NATO Confidential, and all Atomal documents shall be double-wrapped in the same manner as equivalent U.S. classified documents, except that the inner wrapper shall be marked with the appropriate NATO markings. NR information shall, at a minimum, be transmitted in a single opaque envelope or wrapping. There shall be no indication that the contents are classified. NU may be transmitted in a single opaque envelope.
2. Documents classified NATO Restricted shall be packaged in the same manner as NATO Confidential and above. The outer envelope shall be marked, "Postmaster Do Not Forward. Return to Sender."
3. Requirements for the transmission of NATO classified information are contained in USSAN Instruction 1-07.

C. Destruction of NATO Information.

1. All NATO holdings must be reviewed frequently to ensure that the number of documents is kept to the absolute minimum necessary for operational purposes.
2. All NATO classified information must be destroyed in the same manner as prescribed for U.S. classified information in Paragraph 22.7 of this Security Manual. Handling and destruction of the material shall occur by appropriately cleared personnel with NATO access. Destruction certificates and control records for NS information shall be retained in the registry or office performing the destruction for a minimum of five years.

25.8. ADDITIONAL NATO SECURITY GUIDANCE AND NATO MARKING

The United States Implementation of NATO Security Procedures, USSAN Instruction 1-07 Instruction, prescribes the security procedures for NATO information. The OSY maintains a copy of the instruction. Except in those instances where an intelligence source or method would be revealed, portions of U.S. documents containing foreign government information shall be marked to reflect the country or international organization of origin as well as the appropriate classification, for example, NATO-S for a NATO Secret document or UK-C for a Confidential document originating from the United Kingdom. For additional guidance on classification markings, see Chapter 19.

Chapter 26. Foreign Government Information

26.1. CLASSIFICATION

This chapter describes the standards for safeguarding foreign government information other than Northern Atlantic Treaty Organization (NATO) information. Foreign government information (FGI) is information provided to the United States by a foreign government or international organization of governments, or produced by the United States through a written joint arrangement, that requires either the information or the arrangement, or both, to be kept in confidence. The unauthorized disclosure of foreign government information is presumed to cause damage to the national security; therefore, foreign government information shall retain its original classification designation or be assigned a U.S. classification level that will ensure a degree of protection equivalent to that provided by the originator of the information. The authority to assign a U.S. designation to foreign government information does not require Original Classification Authority (OCA).

A. Foreign Government Information.

1. Information provided to the United States 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;
2. Information produced by the United States 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 that the information, the arrangement, or both, are to be held in confidence; or
3. Information received and treated as "foreign government information" under the terms of a predecessor order.

B. Classified or Restricted Foreign Government Information.

1. **Top Secret.** Records shall be maintained of the receipt, internal distribution, destruction, access, reproduction, and transmittal of Top Secret foreign government information. Reproduction of the information requires the consent of the originating government.
2. **Secret.** Records shall be maintained of the receipt and external dispatch of Secret foreign government information. Other records are not necessary unless required by the originator. Secret foreign government information may be reproduced to meet mission requirements.
3. **Confidential.** Records need not be maintained for Confidential foreign government information unless required by the originator.
4. **Restricted.** At a minimum, restricted documents must be stored in locked office space, filing cabinets, desks, or similarly secured containers that will prevent access by unauthorized personnel.

C. **Classified Foreign Government Information (FGI) Provided in Confidence**. Such information shall be provided a degree of protection at least equivalent to that required by the government or international organization which provided the information. Some foreign governments have unclassified information that is protected by law and provided to the U.S. in confidence. Such information is safeguarded under the provision of E.O. 13526. When adequate to protect the information, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Classified information. If the foreign protection requirement is lower than the protection required for U.S. Classified information, the following security guidelines shall be followed.

1. Classified FGI documents shall be provided only to personnel having an established, demonstrable need to know, and whose official duties require access to specific information. Physical control shall be maintained over any material that contains foreign government information to prevent unauthorized access to the information.
2. Individuals being given access to Classified FGI shall be notified of any applicable handling instructions. This may be accomplished by a briefing, and written instructions applying specific handling requirements to the approved cover sheet.
3. Classified FGI documents shall be stored in such a manner to prevent unauthorized access. To the extent practicable, Classified FGI shall be stored separately from other classified information to facilitate its control. To avoid additional costs, Classified FGI documents may be stored in a separate drawer within the same security container.
4. Classified FGI documents shall be transmitted in an approved method for classified information, unless the originating government waives this method. U.S. First Class, Express, Certified, or Registered Mail may be used for Classified FGI that requires modified handling procedures. The use of telecommunications services, including voice facsimile, narrative messages, communication facilities, and radio communications, shall consider security methods available for the transmission of Classified FGI over this form of media. These considerations include, but may not be limited to, physical, administrative, and communications protective features and any other supplemental controls established to provide an acceptable level of protection for Classified FGI. These protective features shall deter access to Classified FGI by unauthorized individuals and restrict public accessibility.
5. Classified FGI that requires modified handling procedures shall be destroyed by using strip cut shredders that result in particles no larger than 1/4-inch wide strips or by using a shredder authorized for the destruction of U.S. classified materials. Such material may also be placed in "For Classified Waste Only" burn bags and destroyed via approved burn methods.
6. When Classified FGI is being considered for declassification or appears to be subject to automatic declassification, the declassifying official shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. Depending on the date of the information and whether it

is contained in permanently valuable records, the declassifying official shall also determine if another exemption identified in the E.O. 13526, Classified National Security Information, applies to the information. If the declassifying official believes such an exemption may apply, he or she shall consult with any other concerned agencies in making the declassification determination. The declassifying agency or the Department of State, as appropriate, shall consult with the foreign government originator prior to declassification.

26.2. DURATION OF CLASSIFICATION

FGI shall be protected for the duration indicated by the originator or source. In the absence of guidance from the originator, follow paragraph 17.6, Duration of Classification under E.O. 13526, for declassification instructions.

26.3. DECLASSIFICATION

A. Declassification authorities can declassify FGI after coordination with the foreign government or international organization of governments that furnished the information or have a written joint arrangement with the United States. In the absence of downgrading or declassification instructions, FGI shall be systematically reviewed in accordance with paragraph 18.7, Systematic Declassification Review.

B. Requests for mandatory review for declassification of foreign government information shall be processed under paragraph 18.8, Mandatory Declassification Review, and must be coordinated with the foreign originator.

26.4. MARKING

A. Foreign government documents may maintain their original markings if they meet the identification purposes served by U.S. classified marking policies (i.e., so that a prudent, responsible individual can reasonably be expected to identify and recognize a document is sensitive and requires special protection and control). Otherwise, FGI documents shall be marked, "C/FGI-MOD" (CONFIDENTIAL FOREIGN GOVERNMENT INFORMATION-Modified Handling Authorized). If remarking a foreign originated document or material is impractical, an approved cover sheet is an authorized option. For specific examples of marking foreign government information, see paragraph 19.9, Other Markings.

B. The written consent of the originating government is required prior to the release or disclosure of any foreign government information to any third-country entity.

Chapter 27. Communications Security

27.1. Communications Security Measures

Communications Security (COMSEC) is the system of security measures used to protect classified National Security Information (NSI) or material using cryptographic keying material and equipment. COMSEC measures are taken to deny unauthorized personnel information derived from telecommunications of the U.S. Government concerning national security and to ensure the authenticity of such telecommunications. COMSEC includes cryptography, transmissions security, and physical security of COMSEC material and information.

27.2. COMSEC Requirements

NSI shall not be discussed over, or otherwise transmitted or processed by, any form of communications unless approved measures are taken to protect the information. Federal COMSEC policies are developed and issued under the purview of the National Security Council (NSC). Implementing instructions are issued by the National Security Agency (NSA). This chapter is intended to implement the NSA security requirements governing COMSEC equipment and operations.

27.3. COMSEC Roles and Responsibilities

A. **Heads of Operating Units.** The head of each operating unit is responsible for providing an appropriate level of security for offices in his or her organization that house or support COMSEC operations or handle information processed and protected by COMSEC systems.

B. **COMSEC Officer.** The Department's COMSEC Officer serves as the principal representative of the Office of Security (OSY) to implement the policies and procedures required to protect and use of cryptographic keying material and equipment in the Department. The COMSEC Officer provides guidance to COMSEC Custodians in the bureaus, operating units, and field offices, to ensure that COMSEC regulations and security measures are planned and implemented throughout the Department. The COMSEC Officer also acts as a Traditional Custodian, providing guidance to hand receipt holders in carrying out their duties and responsibilities.

C. **COMSEC Custodian.** Appointment to the position shall be identified in writing by the NSA. COMSEC custodians will be assigned to a Traditional or a Seed Only COMSEC Account (SOCA) depending on the type and amount of cryptographic equipment under their control.

1. COMSEC Custodian (Traditional) – The traditional custodian provides guidance to operating units and hand receipt holders, in their area of responsibility, to ensure that COMSEC regulations and security measures are planned and implemented. The traditional custodian is responsible for maintaining up-to-date records and submitting required accounting reports to the NSA. Traditional custodians are also responsible for administering and/or providing the initial user education briefing and

cryptographic briefing (for other traditional custodians or COMSEC repair technicians). Traditional custodians shall maintain copies of all briefings. Traditional custodians shall also undergo required NSA COMSEC custodial training, within six months of appointment.

2. COMSEC Custodian Seed Only Account (SOCA) – SOCA custodians can only maintain, order, and safeguard seed keys within the account. SOCA custodians, if necessary, will provide guidance and user education briefings. NSA COMSEC custodial training is not required for SOCA custodians.

3. Any changes (custodian, account type, etc.), or violations in Departmental COMSEC accounts (Traditional or SOCA) shall be reported to the Department's COMSEC Officer, in OSY.

D. Alternate COMSEC Custodian. In the absence of a COMSEC Custodian (Traditional or SOCA), a designated alternate COMSEC Custodian shall perform all the duties noted above for offices and/or operating units in their area of responsibility. Appointment to the position shall be identified in writing by the NSA, and COMSEC custodial training is required within six months of appointment for traditional custodians.

E. Individual User. Each individual user is responsible for ensuring appropriate COMSEC equipment is used when communicating NSI over telecommunications lines. In addition, each user must verify the security clearance and need-to-know of the recipient of the information. Personnel are prohibited from discussing NSI on a secure phone when the telephone is not placed in secure mode. Prior to COMSEC access, each user shall receive a COMSEC user education briefing.

F. Hand Receipt Holder. The Hand Receipt Holder signs for COMSEC materials in a particular office, operating unit, or bureau, and ensures monitoring, safeguarding and controlling of such materials.

27.4. COMSEC INVENTORIES

All departmental COMSEC accounts have the ability to affect the viability of other accounts, and therefore, the department's COMSEC Officer (in OSY) shall provide oversight to operating units and shall require validation of inventories to ensure that each designated custodian and hand receipt holder complies with NSA regulations in the proper monitoring, controlling, and safeguarding of COMSEC material and equipment.

A. COMSEC Custodian (Traditional) – shall provide oversight to operating units and shall conduct semi-annual equipment inventories to ensure that each designated Hand Receipt Holder complies with NSA regulations in the proper monitoring, controlling, and safeguarding of COMSEC material and equipment.

B. COMSEC Custodian (SOCA) – shall provide oversight to operating units and conduct annual equipment inventories to ensure that each designated Hand Receipt Holder

complies with NSA regulations in the proper monitoring, controlling, and safeguarding of COMSEC material and equipment.

27.5. REPORTING COMSEC SECURITY VIOLATIONS

Specific guidance for reporting COMSEC security violations is contained in NSA Manual 3-16, *COMSEC Material Control Manual.* All violation reports termed "insecurities" by NSA in this manual shall be reviewed by the servicing security office prior to forwarding to the Department's COMSEC Custodian in OSY.

Chapter 28. Classified Information Systems

28.1. IT Security Requirements

The Department of Commerce (DOC) requires all operating units to implement and maintain an information security (IT) security program consistent with federal laws and regulations and departmental policies, procedures, and standards. IT security operations are designed to protect and defend the availability, integrity, and confidentiality of information and information systems. Operating units must establish protection, detection, and reaction capabilities to restore an information system in the event of an intrusion or system failure. Operating units that have a need to process or store classified National Security Information (NSI) shall have each IT system certified and accredited prior to processing or storing classified information.

The National Security and Telecommunications Information System Security Instruction No. 1000 (NSTISSI No. 1000) describes the process used to certify and accredit IT systems. The *National Information Assurance Certification and Accreditation Process* (NIACAP) described in this document shall be used as the process for accreditation of classified systems in the DOC.

Additionally, the DOC Information Technology Security Program Policy (ITSPP) specifies the mandatory requirements for the DOC IT Security Program, which encompasses controls to be implemented on information systems. This policy addresses requirements and guidance set forth by the Federal Information Security Management Act (FISMA) and provides clarity on the Department's specific control parameters. It also encompasses minimum security controls as required by Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, and defined by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 , Revision 2, Recommended Security Controls for Federal Information Systems, commensurate with the security categorization defined by FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

28.2. Periodic Review of Systems

Systems processing classified NSI shall be reviewed every three years for certification and accreditation or when major changes are made to the system. System owners shall contact the appropriate Designated Approving Authority (DAA) (see below) to coordinate the review and accreditation process no later than the third anniversary of the original certification (or earlier if necessary) to ensure each system processing classified information is accredited.

28.3. Roles and Responsibilities

This paragraph describes the roles and responsibilities of the Department, operating units, program offices, and individuals responsible for safeguarding classified NSI on IT systems processing or storing classified information.

A. **Heads of Operating Units.** As the system owner, the head of each operating unit is responsible for ensuring that his or her systems are certified and accredited prior to processing or storing classified information. The head of an operating unit shall designate approving authorities and information technology security officers (ITSO) for his or her organization. The name of the ITSO for each operating unit and/or sub-unit will be submitted in writing through the Servicing Security Officer to the Office of Security (OSY). The ITSO shall ensure that system owners properly maintain their respective system's security throughout the system's life cycle.

B. Designated Approving Authority.

1. The head of each operating unit shall appoint one or more DAAs. The DAA has the authority to review and accredit information processing systems in his or her respective organization. The DAA will ensure a systems certification team reviews each IT system prior to accreditation. Managers of systems that process classified information shall contact their operating unit's DAA to arrange for system certification and accreditation.
2. The DAA grants formal accreditation to operating systems processing classified NSI. The DAA has the authority to suspend operations, grant interim approval to operate, or approve variances. The approval will be in writing and shall be included in the System Security Plan Certification and Accreditation Package (SSCAP), which is the format used by the Department in place of the Systems Security Authorization Agreement (SSAA) suggested by the NIACAP.
3. The DAA shall report the findings of security violations and incidents involving classified IT systems to the Director for Security (Director) and the Department DAA.

C. **IT Security Program Manager.** The Department Chief Information Officer (CIO) is delegated the responsibility to develop Department-wide policies, procedures, and other directives for IT security, including classified systems. The IT Security Program Manager serves as the principal representative of the Office of the CIO to manage and implement the Department's IT Security Program. The IT Security Program Manager provides support to operating units to ensure that IT security safeguards are planned and implemented throughout the life cycle of the classified IT systems in the Department. The IT Security Program Manager shall perform the following tasks:

1. Provide support to operating units conducting system certification and support each operating unit's DAA in system accreditation.
2. Review documentation of classified IT systems for completeness and accuracy.
3. Consult with the OSY regarding physical and personnel security of classified systems.
4. Ensure that policies and procedures are in place to require security testing and evaluation of classified IT systems in support of the certification process.
5. Establish requirements for the Security Education and Awareness Training program activities pertaining to classified IT systems security.

D. **Operating Unit IT Security Officer.** The ITSO for each operating unit shall be responsible for assisting the system certification team in collaboration with the OSY. The ITSO shall perform the following tasks:

1. Develop and monitor implementation of IT system security policies and procedures for classified systems, including preparation of system security plans and procedures for clearing, purging, declassifying, and releasing system memory, media, and output.
2. Assist in the system's security certification, inspections, tests, and reviews.
3. Ensure that the proper notifications are made and corrective actions are taken when a system incident or vulnerability has been discovered.
4. Investigate security violations and incidents involving classified IT systems and report the findings to the DAA and to the OSY.

E. **IT System Owner.** The IT system owner shall perform the following tasks:

1. Ensure that systems under his or her responsibility are certified and accredited.
2. Maintain the SSPCAP, which includes all system documentation for each classified system.
3. Ensure that all users have the appropriate security clearances and authorization, and that they are familiar with the system security plan and their security responsibilities prior to receiving access to the information system.
4. Develop an evaluation process to assess changes in a classified IT system and its operating environment and the operational needs that could affect the accreditation.

SECTION IV. PHYSICAL SECURITY

Chapter 29. Physical Security Program

29.1. PURPOSE

The Manual of Security Policies and Procedures (the manual) implements the policies and procedures that govern the management and administration of the personnel, facilities, material assets, information, infrastructure (e.g., cyber, electrical, telephonic) and physical security programs of the Department of Commerce (Department). Chapter 40 (Anti-Terrorism Risk Assessment Program) of the manual prescribes the policies, procedures, and standards that govern the implementation of physical security measures designed to protect personnel, facilities, property, and information in the Department. The manual also specifies the minimum physical security standards for the Department.

29.2. APPLICATION

A. The physical security policies and procedures described in this manual apply to all Departmental operating units, offices, facilities, employees, visitors, on-site contractors and associates, and others who have access to or use Departmental facilities and assets. Provisions in this chapter take precedence over physical security policies of any bureaus, operating facilities, or other offices in the Department; however, nothing in these regulations shall be construed as contrary to the provisions of any statute or Federal regulation. In the event of conflict, specific statutory provisions shall apply.

B. The senior official or manager of each operating unit, office, or facility in the Department is responsible for the safety and security of his or her personnel, property, and information. Managers have certain specific security responsibilities that are described in this manual. In addition, each employee is responsible for adhering to the security requirements prescribed in this manual. Employees or other personnel associated with the Department shall report any incident or condition contrary to these requirements to their Security Contact, Servicing Security Office (SSO), or the Office of Security (OSY).

C. Requests for exemptions from the provisions of the physical security requirements for inspections and surveys may be made to the Director for Security (Director) to address unusual situations to specific organizations. A request for an exception must be made in writing and must set forth the justification and proposed compensatory measures for safeguarding or affording equivalent protection for the persons, property, or facilities involved.

D. Failure to comply with the Department's physical security policies, regulations, or procedures may result in administrative or criminal sanctions, including withdrawal of security clearance and disciplinary action that could range from counseling to removal from Federal service. Violations of a criminal statute shall be reported to the Office of Inspector General for possible referral to the Department of Justice.

29.3. PHYSICAL SECURITY POLICIES

A. To ensure the protection of Departmental personnel and assets, physical security programs shall be established and implemented in each operating facility based on the minimum standards set forth in this manual and other appropriate laws, regulations, and national codes for the protection of life and property. These programs shall be administered and monitored continually to ensure their integrity. All security standards will be met in new facilities whether constructed or acquired by purchase or lease. Every attempt will be made to acquire sites or new facilities that meet physical security standards. In the event that one or more standards are not met for a specific building, the Physical Security Criteria for Federal Facilities provides guidance for accepting risk.

B. Operating facilities on Federal property under the control of the General Services Administration (GSA) and that hold a security delegation of authority from GSA must provide for the security and protection of personnel and assets within the property. Based on the Presidential Policy Memorandum, Upgrading Security at Federal Facilities, dated June 28, 1995, the head of the operating facility shall upgrade and maintain security in owned or leased facilities under his or her jurisdiction to the minimum standards specified in the Department of Homeland Security, Interagency Security Committee (ISC) Facility Security Level (FSL) Determinations for Federal Facilities, dated January 14, 2008, and the ISC Physical Security Criteria for Federal Facilities, dated April 12, 2010. Physical security surveys and Anti-Terrorism Risk Assessments (ATRA) address the criticality of operations, the vulnerability of the facility or area, and the probability of loss or damage to facilities or property and danger to personnel. The SSO shall assist the facility manager in developing a security plan for addressing any recommendations resulting from the surveys, inspections, or self-administered checklists. All recommendations shall be coordinated with OSY.

Note: The ISC FSL uses Roman numerals while the Department uses Arabic numbers to identify facility levels.

C. The extent of exterior and interior controls will be determined by considering the local threat assessment, mission criticality, vulnerability of the facility, monetary value of the items or areas to be protected, and the cost of the controls. Normally, the cost of security controls should not exceed the value of the item or area to be protected.

D. A restricted area requires special restrictions or controls to safeguard property or material. Admittance to a restricted area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area. Personnel without an appropriate security clearance must be escorted in a restricted area where Classified National Security Information is produced, processed, or stored by personnel assigned to the area. When un-cleared personnel are present in a restricted area, NSI must be protected from observation, disclosure, or removal. The Security Contact or office manager is authorized to designate an area as a restricted area after adequate security measures are in place.

E. Each employee, contractor, or associate of the Department is required to possess and carry a form of identification (ID) while in duty status and will be subject to local restrictions prescribed by the facility manager. All personnel in facilities identified as Level II, III, and IV require agency photo ID that is worn and visible at all times when in government-controlled space. The displaying of a photo ID in Level I facilities is recommended.

F. Forms of ID shall be restricted to those critical to the accomplishment of the Department's missions. Special forms of ID for unique purposes or special facilities require justification. An example is the Census Bureau's enumerator ID for special censuses. Any proposal for a new form of ID shall be submitted in writing with a detailed justification through the SSO to OSY for approval.

G. Any person within a facility, regardless of position, shall be subject to challenge by another person, the servicing guard force, SSO, or any law enforcement officer, and shall display appropriate identification when challenged. Failure to do so may result in removal from the facility or other administrative action.

H. DOC facilities house a wide variety of functions and activities that are performed by Federal Government employees, Departmental associates, official visitors, foreign nationals, and the general public. Access to Departmental facilities during and after business hours shall be controlled as specified in local security procedures. Policies and procedures for access to local Departmental facilities shall be established by the ranking unit official or senior facility manager and shall comply with the policies and minimum standards set forth in this manual. Decisions on admittance policy shall take into consideration the sensitivity of the facility; the criticality of the operations; existing access controls (including guard forces and their response capability and alarm systems) and the investigative process completed on the persons who will have access.

I. Level I facilities are normally open to the public for official business during regular business hours; however, access is restricted after business hours to protect Departmental assets. Level II facilities require visitors to non-public areas be sponsored by a tenant and either approved for unescorted access or escorted at all times. Level III and IV facilities require visitors to non-public areas be sponsored by a tenant and either approved for unescorted access or escorted at all times; visitors in non-public areas are in addition, required to display a visitor ID badge. Security hours are those hours a facility is closed to the general public where access must be limited to individuals essential to the official business of the Department. The facility manager shall coordinate with OSY and/or the SSO for implementation of access controls for Department facilities during security hours.

J. Non-employees, such as visitors and family members, may be admitted to facilities subject to local procedures developed by the facility manager and the SSO, provided such visits do not disrupt the normal business of employees. Facility managers and/or SSOs may use a registration form or other written record to obtain an employee's acknowledgment of this responsibility. Areas may be closed to public access when

circumstances require action to ensure the orderly conduct of government business. The decision to close public areas shall be made under GSA Federal Management Regulations or local requirements in consultation with appropriate security officials.

K. When forms of ID are required for admittance to Departmental facilities, employees or maintenance and contractor personnel shall display an authorized form of ID at all times. Some Departmental facilities may be closed to employees, contractors, and other persons as special circumstances warrant. During such special restrictions, supervisors may need to provide lists of essential persons to the facility manager or security officials to arrange authorization for employees, contractors, or other persons to enter the facility. A completed CD-165, Admittance to Department Facilities During Security Hours, or a memorandum may be used for this purpose. Union representatives will normally be granted access to their union offices and files if conditions allow.

L. All access control procedures shall be established in accordance with the standards prescribed in the ISC Physical Security Criteria for Federal Facilities, dated April 12, 2010. If necessary, the facility manager may strengthen the access control procedures in this manual. On the other hand, to accommodate unusual operations, facilities, or circumstances, local officials may prescribe less restrictive admittance procedures, provided they are within the guidelines established by the ISC Physical Security Criteria for Federal Facilities, dated April 12, 2010.

M. Personnel should immediately report missing office keys to the issuing office. The SSO should conduct a security evaluation to determine whether it is necessary to re-key the office. Security Contacts, facility managers, or other issuing officials should allow a reasonable waiting period before the replacement of lost keys. The waiting period will allow time for a lost key to be found before expending the time and expense of issuing a replacement. The ISC Physical Security Criteria for Federal Facilities, dated April 12, 2010, establishes further guidance for key control and access media accountability.

N. With the exception of contract security officers, all positions in the Department encumbered as police officers or law enforcement officers (LEO) and required to carry firearms in the line of duty will be designated High Risk at a minimum and will be processed in accordance with Chapter 10, Position Designation, of this manual. Police officers or LEO personnel occupying a position that requires access to NSI will; at a minimum, be designated Critical-Sensitive. Special Departmental investigative processing is required for contract security officers and certain other precautionary measures must be taken by selecting facility and security officials to reduce the possibilities of mishaps involving firearms.

O. Security containers used for the storage of NSI shall be controlled by the Security Contact in an operating facility in consultation with the SSO and, Counterespionage Division (CED). Records of security container use shall be maintained in the Department's electronic database system, Security Manager. If an operating unit or other Departmental office does not have access to the system, appropriate records, electronic or written, shall be maintained by the SSO or the Security Contact to ensure the

accountability of security containers. The classified control point in each operating facility is responsible for recording information into Security Manager.

P. Before procuring new storage containers, managers should make an effort to retire, return, declassify, or destroy unneeded NSI to make storage space or containers available. Managers shall also check with property management personnel to determine whether surplus containers are available prior to purchase of new containers.

Q. A large number of filing cabinets with security lock-bars and padlocks in the Department have been conditionally approved for classified storage up to the Secret level. However, lock-bar filing cabinets are easily compromised and do not provide adequate protection for NSI. Therefore, these containers must be phased out of use by October 1, 2012. Until October 1, 2012, material up to the Secret level may be stored only if the equipment is already in use. These cabinets must be systematically phased out and be replaced with newer GSA-approved security containers.

R. Volumes of valuable and critical property pass through shipping and receiving areas daily. Managers often create areas for the storage of new or used equipment waiting for distribution. If not properly protected, the areas become vulnerable to theft and misappropriation of the stored equipment. Storage areas should be located away from shipping and receiving areas and facility entry and exit points to make the unauthorized removal of stored items more difficult.

S. Procedures shall be established for the control of incoming property, and shipments shall be checked for signs of pilferage or damage. A careful inventory of incoming shipments shall be conducted to assure that all items on the bill of lading or other manifests are received. Delivery records should be checked against requisitions and purchase orders. Only designated personnel who have been determined to be trustworthy shall be authorized to accept or sign for deliveries. Damaged merchandise should be separated and secured until disposition can be made. Instruct personnel not to leave unscreened mail and packages next to columns surrounding the mail screening and receiving area or against walls abutting critical areas.

T. GSA regulations require that all property leaving Federal facilities be accompanied by proof of authorized possession or ownership. The form presently in use in the Department for this purpose is the Optional Form 7, Property Pass. Each bureau must designate a property custodian in writing to coordinate all property leaving the facility. The duration of the Optional Form 7, Property Pass, will depend on the individual or organizational requirements.

U. Automated information systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft; alteration; damage by fire, dust, water, power loss and other contaminants; and unauthorized disruption of operation. The extent of physical security measures needed is determined by the results of a risk assessment and/or a physical security survey.

V. At a minimum, computer facilities should be designated as controlled areas. A major computer facility shall be designated as a restricted area in which access into the facility is limited to personnel who are assigned there or who are authorized access by the facility manager.

29.4. PHYSICAL SECURITY PLANNING

A. Senior managers responsible for Departmental facilities shall ensure that security planning is an integral part of any function or project undertaken within the Department. Selecting, constructing, or modifying a facility without considering the security implications of employee safety and asset protection can result in costly modifications or retrofitting, considerable lost time, and liability for the Department.

B. All security standards will be met in new or altered facilities whether constructed or acquired by purchase or lease. Every attempt will be made to acquire sites or new facilities that facilitate meeting physical security standards. In the event that one or more security standards are not met for a specific building, the Physical Security Criteria for Federal Facilities provides guidance for accepting risk.

C. Physical security programs shall be established and implemented within each operating facility based on the minimum standards set forth in this manual and other appropriate laws, regulations, and national codes for the protection of life and property to ensure the protection of Departmental personnel and assets. The programs shall be administered and monitored to ensure their integrity. At a minimum, a facility physical security program shall include all of the following elements:

1. An ATRA for each owned or wholly leased facility occupied by Departmental personnel.
2. Scheduled/unscheduled inspection of facilities to determine whether the local security program meets required Federal and Departmental standards or regulations.
3. A comprehensive and continuing security education and awareness effort to gain the interest and support of employees, contractors, consultants, and visitors.
4. An established process of emergency procedures to take immediate, positive, and orderly action to safeguard life and property during an emergency.
5. An appropriate set of security procedures to respond to changing threat conditions.

D. The ATRA will evaluate the capability of the facility to protect Departmental personnel, assets, and information. The interior and exterior portions of a facility should be recorded using digital video recording (DVR) or videotaped for the record.

29.5. FACILITY PROTECTION

A. The senior facility manager shall determine the level of protection required for each facility under his or her control based on the results of a comprehensive ATRA of the facility. The ATRA will identify the jurisdictions involved and required responses. Formal agreements with local protective service companies or law enforcement agencies

may be required to ensure proper responses. At a minimum, a facility physical security program shall use a layered security or defense-in-depth approach consisting of the following criteria:

1. Perimeter protection is the first line of defense in providing physical security for personnel, property, and information at a facility.
2. Interior controls, as the second line of defense, are perhaps the most important. The extent of interior controls will be determined by considering the local threat environment and criticality of the items and areas to be protected, the vulnerability of the facility, monetary value, and the cost of the controls necessary to reduce that vulnerability.
3. The cost of the security controls normally should not exceed the monetary value of the item or area to be protected unless necessitated by criticality, loss of human life, or national security.

B. Departmental facilities that handle, store, or process Top Secret NSI are required to employ guard services or other appropriate response forces to protect that information. Contract guard services may be provided at other Departmental facilities after coordination between the facility manager and the SSO. An ATRA of the facility will determine the type and size of guard service. Any new security guard requirement shall be supported by an ATRA.

29.6. PLANNING FACILITY PROTECTION

A. The objective of planning facility protection is to ensure both the integrity of facility operations and the security of personnel, property, and information. Security requirements must be integrated into the site selection and construction or renovation before moving into a Departmental facility.

B. The modification of a facility or addition of security measures after occupying a facility can be costly and impractical; therefore, the facility manager and the SSO shall define the security measures necessary to support the facility's mission and work prior to any construction or renovation. Coordination shall begin with the designers and architects and continue through the contracting process and construction and installation.

C. Many Departmental offices occupy space in commercial buildings where GSA executes the lease for the Department. In leased office space with multiple tenants, access may not be controlled to the same extent as in a facility where the Department is the sole tenant. When the Department is the sole tenant, the Security Contact has more flexibility to plan and implement access controls. In most multi-agency tenant buildings, Departmental tenants must rely on GSA to provide protection for the building. When GSA provides security, Departmental Security Contacts and administrative officials must establish a working relationship with the appropriate GSA officials and maintain an active role in the security decisions and processes that affect the facility.

29.7. DESIGN FACTORS

A. Introduction. Security systems and procedures shall be considered from the original design stage to the completion of the project. Metal conduit runs, alarm wiring, utility access, reinforcing devices, and other necessary construction requirements should be included in the original design and construction plans. Factors for consideration are as follows:

B. Facility and Building Location.

1. **Access Requirements.** The planner must review the mission of the facility and determine the level of public access permitted, response times of security personnel to incidents during duty and non-duty hours, and the workflow and processes so security can be integrated into the facility.
2. **Geographical Factors.** The planner must consider approach routes, traffic patterns, and nearby transportation. If possible, facilities should not be located near high-crime, high-traffic, or industrial areas.
3. **Building Configuration.** At a facility site, the number of separate buildings should be kept to a minimum and grouped close together. Close-in access for vehicles shall be discouraged. Barriers or passageways should be constructed to permit employees and property to pass safely between buildings.

C. Configuration of Space.

1. **Entrances.** Facility or office entrances should be kept to the absolute minimum, yet comply with fire safety codes. Although employee access, parking, and deliveries are to be accommodated, security-maintained entrances shall be engineered with provisions for guard posts and access control systems. One entrance with multiple interior routes is preferable to several outside entrances. Plans shall include space for reception desks, barriers, and other controls.
2. **Lock and Key Control.** High security locking devices shall be used on all perimeter doors, and locking devices shall be used on all interior doors. The locks can either be key lock devices or electronic access control systems for entry. Cleaning, maintenance, and protective staff need access to do their jobs. Keys, Personal Identification Numbers, and time periods shall be defined to support these functions.
3. **Location of Offices and Facilities.** Offices or other facilities should be adjacently located and on the same or successive floors. Facility managers should try to avoid leasing space that has non-Departmental-leased space between Departmental-leased spaces. Sensitive operations such as credit unions, imprest funds, or those involved in handling NSI or sensitive information should be located on upper floors and away from entrances. Related activities, such as shipping and receiving, should be located in adjacent or nearby locations. To control access to the spaces, facility managers shall install locks on entrances, exits, and corridor doors. Perimeter doors and

interior rooms will be locked when unattended. Key issuance and control programs must be established.

4. **Contract Guard Forces.** Access controlled by a contract guard force requires written procedures to define who can enter the facility. When a guard service is not used or available, facility managers shall establish a liaison with local law enforcement officials and advise them of the security hours and emergency contact information. If necessary, facility managers shall arrange for the protection of employee parking areas.

5. **Property Control.** Facility managers shall establish procedures to provide for the control and removal of property, equipment, and official records. Signature exemplars of property pass holders must be maintained on file and used by the contract guard force to control improper removal of property, equipment, and official records.

D. Safety and Fire Protection. Safety and fire protection requirements must be incorporated into any construction plans. Operating facilities must follow accepted fire prevention practices in operating and managing buildings. Federally owned buildings are generally exempt from state and local code requirements in fire protection. In accordance with Title 40 USC Sec 3312 (Compliance with nationally recognized codes), however, each building constructed or altered by a Federal agency must be constructed or altered, to the maximum extent feasible, in compliance with one of the nationally recognized model building codes and with other nationally recognized codes. Operating facilities in the Department must use the National Fire Prevention Association (NFPA) codes and standards as a guide for their building operations. Managers shall contact GSA and/or appropriate officials regarding GSA requirements, NFPA codes, and possible local code requirements and construction standards when constructing or altering Federal facilities.

E. Utilities. Utility systems shall be protected against unauthorized access. The protection of telephone, electrical, heating and cooling systems, water supplies, boilers, generators, valves, regulators, and controls must be planned.

F. Special Activities. Special emphasis shall be placed on security systems and safeguards when constructing or modifying special or sensitive activities such as mailrooms, equipment storage or shipping and receiving areas, classified work areas, computer rooms, childcare centers, and special use areas such as warehouses or hazardous materials storage areas.

G. Contingency Plans. A contingency plan must be developed for each Departmental facility to protect personnel and property in the event of emergencies such as fire, bomb threats, civil disturbances, and natural disasters. See Chapters 39 and 7, respectively, within the manual.

29.8. ANTI-TERRORISM RISK ASSESSMENTS AND PHYSICAL SECURITY INSPECTIONS

A. **Introduction.** An ATRA is an in-depth analysis used to determine security measures needed to protect Departmental personnel, property, and information. An inspection is a check or test against a set of standards or regulations to verify that a security program or facility meets those standards or regulations. Inspections evaluate implementation of regulations, the education of employees, security administration, and existing internal management controls. The facility manager shall use surveys and inspections to carry out oversight responsibilities. (See Chapter 40, Anti-Terrorism Risk Assessment Program).

B. Anti-Terrorism Risk Assessments.

1. **Purpose.** The facility manager, in conjunction with the SSO, will assess the local threat environment and conduct an ATRA of each owned or wholly leased facility under his or her jurisdiction to determine the type and extent of security controls necessary for each facility or area. Each ATRA will include a security evaluation that addresses the criticality of operations, the vulnerability of the facility or area, the probability of loss or damage to the facility or property and danger to personnel, and recommended countermeasures presented on a cost-benefit basis.

2. **Recommendations.** The SSO shall assist the facility manager in developing a security plan to address recommendations resulting from the surveys, inspections, or self-administered checklists. All recommendations shall be coordinated with OSY.

3. **Threat, Criticality, Vulnerability, and Probability of Risk.** An ATRA is not complete until the factors listed below have been given full consideration:

   a. **Threat Assessment.** A threat assessment evaluates the potential aggressors and the type of tactics that they are most likely to employ. The threat assessment should consider a complete spectrum of threats, including natural (e.g., earthquakes, floods, fires, tornados, hurricanes, etc.) and man-made (e.g., accidents, criminal acts, terrorist acts, etc.). For threats involving explosives and other weapons of mass destruction, the threat assessment should quantify the type and/or size of device. The result of the threat assessment is a list of credible threats and/or attack scenarios.

   b. **Criticality.** Criticality defines the effect that work reduction or mission loss would have on a facility or operation. Work loss or reduction could have a negative impact on national security, Departmental mission, or a facility's operations. Examples of adverse effects include the interruption of a vital function, disruption of operations, or the compromise of NSI. A higher classification level of information processed or stored in a facility will increase the *impact of loss* factor at that facility.

   c. **Vulnerability.** Vulnerability describes the susceptibility of a facility or operation to damage, destruction, possible theft, or loss of property. Physical vulnerability factors include the size, configuration, construction, and location of the facility.

Area vulnerability factors include population demographics, the local crime rate, the proximity of law enforcement, and emergency response services.

d. **Risk.** Risk evaluates the potential for damage or loss to a Departmental operation, activity, facility, or mission. A risk assessment is conducted to determine the probability that an action, circumstance, or event could cause loss or damage to a Departmental asset. Probability of risk is an ever-changing dynamic that depends on the intention and capability of an adversary to undertake actions detrimental to Departmental interests.

4. **Types of Anti-Terrorism Risk Assessments.**

   a. **Initial ATRA**. The initial ATRA is conducted prior to constructing, leasing, acquiring, modifying, or occupying a facility or area. It identifies security measures or equipment necessary to maintain the level of security required to protect the facility dictated by the criticality and vulnerability of the facility.
   b. **Compliance ATRA**. After the initial ATRA, a compliance survey is conducted to ensure the completion of specified modifications. This survey shall be conducted before acceptance of the property or occupancy.
   c. **Supplemental ATRA.** A supplemental ATRA is conducted when significant changes in organization, mission, or facility structure occur. The ATRA is conducted at the discretion of either the facility manager or the SSO.

5. **Conducting ATRAs**. The SSO shall conduct an ATRA with the assistance of the facility manager. The facility manager will provide a layout of the facility depicting interior areas in the facility, access points, parking lots, warehouses, and any adjacent areas belonging to the facility. The SSO shall interview program management officials to determine the mission and nature of operations, classification or sensitivity level of information, and value of assets. He or she should visit the facility or area to obtain the information noted below:

   a. The facility's address, number of buildings, tenant organizations, approximate population, and names of key management officials.
   b. The security level of the building as determined by the Facility Security Level Determinations For Federal Facilities: An Interagency Security Committee Standard, dated January 14, 2008.
   c. Type of construction of buildings at the facility.
   d. A description of features of the facility and conditions that produce vulnerabilities. The physical configuration of the office or facility storing NSI shall be documented.
   e. A description of adjacent buildings that could provide access to the facility.
   f. A description of the surrounding area (e.g., types of buildings, terrain, vegetation, roadways, pedestrian walkways, parking lots, etc.) for at least one-quarter mile in all directions. The area should be expanded if significant crime demographics are developed.
   g. An analysis of criminal and fire incidents for the jurisdiction(s) in which the facility is located covering at least a 1-year period. Crime and fire records

should be obtained for the surrounding area of the facility and compared with the facility records.

h. The law enforcement agency, fire department, contract guard force company or agency, and other organizations responsible for emergency response along with its response time.
i. An assessment of the replacement and/or intrinsic value of assets and sensitive or unique equipment. The highest classification level of information processed or stored in the facility and the number and types of weapons should be documented.
j. A description of access controls, alarms, guard services, and security containers.
k. Recommendations for improving security and pertinent implementing instructions.

6. **ATRA.** The SSO, in coordination with the facility manager, will ensure that the ATRA is thorough and precise. The ATRA shall be submitted to the facility or office manager for review prior to completion of the recommendations. A copy of the "DRAFT" ATRA is forwarded to OSY Anti-Terrorism Division (ATD) for review, coordination, and final distribution. The ATRA should include all of the following:

a. The rationale for the ATRA.
b. A security evaluation.
c. A background or history, if applicable.
d. A paragraph describing the environment around the facility.
e. A detailed statement of findings and recommendations for making any necessary security improvements.
f. The exhibits supporting the report such as floor plans, photographs, and specifications.

C. Physical Security Inspections and Surveys

1. **Purpose.** Inspections and surveys, announced or unannounced, are conducted to determine the extent of compliance with security regulations and procedures to ensure the protection of the Department's assets. The facility manager will periodically conduct self-administered inspections of facilities and programs under his or her jurisdiction as necessary to ensure compliance with the provisions of the manual. OSY will provide oversight through a compliance review and assistance visit conducted by the SSO or OSY Compliance Review Team which is comprised of CED, ATD and the Client Services Division. The inspections will result in a written report with copies retained at the inspection site and with the SSO. The surveys will result in an accreditation letter with copies retained at the surveyed location, with the SSO.

2. **Recommendations.** The OSY Compliance Review Team will assist the facility or office manager in resolving any discrepancies or implementing any recommendations.

3. **Types of Inspections.**
   a. **Evaluative or Fact-Finding Inspection.** Promotes a positive tone, while taking a broad, general look at a facility or program. The inspector has the option to resolve the deficiency on the spot or recommend further corrective actions within a non-specified time frame. The evaluative inspection can assist management officials in planning or upgrading their security programs.
   b. **Compliance Inspection.** Focuses on compliance with established standards or regulations and may be admonitory in tone.
   c. **Penetration Inspection.** A deliberate attempt by security officials to breach security systems and procedures to test compliance with regulations and procedures. This type of inspection is usually conducted for counterintelligence purposes at facilities where highly classified and/or critical operations or materials are at risk from hostile intelligence operations. A penetration inspection must be approved, in advance, by the Director.
   d. **Self-Inspection.** Initiated by the facility manager or security contact to evaluate his or her own security program. The initiator determines the scope and purpose of the self-inspection. Further guidance on self-inspections can be obtained from the SSO, facility manager, or OSY.

4. **Frequency of Inspections.** The frequency of inspections will be based on the criticality and vulnerability of a facility or the level of classification or value of information processed or stored at a facility.

5. **Conducting Inspections.** The following guidance provides the minimum steps for conducting inspections:
   a. The inspector shall determine the scope, type, and method of inspection. The inspection must be scheduled with the office or resident facility manager, and if appropriate, written notice shall be provided. The notice should provide the dates, purpose, proposed interview schedule, and a request for any additional information, as needed. The inspector should review past inspection reports and mission statements and prepare a list of questions or a checklist to structure the inspection.
   b. Upon arrival at the site and prior to departure, the inspector shall meet with the Security Contact and the facility manager or his or her representative to discuss the inspection. A sufficient sampling of data shall be collected from interviews with on-site employees and contractors and from touring the facility. The inspector will review the facility's local security procedures. After the review, the inspector shall report all findings, including any discrepancies corrected on the spot.
   c. After sufficient data is collected, the inspector should analyze all findings, compare them with applicable security regulations, list discrepancies and cite regulatory references, recommend corrective actions, and write the inspection report.

d. The inspection report shall be produced within 30 working days of completion of the inspection. It should be divided into sections consisting of a summary, introduction, scope and purpose, overview and methodology, findings and recommendations, and observations. The report should be distributed to the Security Contact and the manager of the facility inspected in a timely manner. The report will require a response to any recommendations no later than 45 working days from the date of report.

6. **Frequency of Physical Security Surveys.** A survey will occur every three years for areas that have/require communications security to include: Secret Internet Protocol Router Network access, classified systems, and open discussion of NSI up to the Top Secret level. After the initial survey, OSY CED will follow-up annually with the client to verify that there have been no changes to the area.

7. **Conducting Physical Security Surveys.** The surveys adhere to a Certification and Accreditation process in which the OSY Compliance Review Team works together to certify and accredit a secure area for NSI. The survey is conducted in accordance with Department Security Policies, Title 32 Code of Federal Regulations, and specifications from the Intelligence Community Directive 705, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities (ICS-705-1) and Standards for Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities (ICS-705-2) and supercedes Director of Central Intelligence Directive (DCID 6/9).

   a. The survey must be scheduled with ATD, and if appropriate, written notice shall be provided. The notice should provide optional dates, systems in/requested for the area, locations, point-of-contact and alternate, and a request for any additional information, as needed. The required documentation is due prior to the survey.
   b. Upon arrival and prior to departure, the assessor shall meet or consult with the OSY Compliance Review Team to discuss the physical barriers and structure of the facility, intrusion detection systems, NSI storage containers and received documentation.
   c. After the survey, ATD will create a written report outlining the observations and recommendations. Once all the findings have been rectified and reviewed by the OSY Compliance Review Team, a certification letter will be created and presented to CED.
   d. CED will review the certification letter with the submitted documentation. CED will then create an accreditation letter to the Director of the area or the SSO.

Chapter 30. Facility Protection

30.1. Perimeter Security Measures

The goal of a security system is to deploy security measures to eliminate or mitigate the potential for criminal and terrorist incidents. The layered security concept emphasizes the need to think of physical security as a system that provides "defense-in-depth." In some cases, defense-in-depth can be obtained by constructing "islands" of extreme or high security within a "sea" of moderate security. This concept is also known as "enclaving." Assets critical to the Department of Commerce (Department) should be protected such that they are located within an innermost ring of security. Additional layers of security are provided at increasing distances from the asset to be protected. The number of layers, the components that comprise them, and their resistance to penetration depend on the threat and the importance of the asset to be protected. Paragraph 30.21 contains the Department's Facilities Security Checklist.

A. Perimeter protection is the first line of defense in providing physical security for a facility. This can be accomplished by installing fences or other physical barriers, outside lighting, lockable gates, intrusion detectors, or a contract guard force. Perimeter protection also includes walls, lockable doors and windows, bars and grilles, fire escapes, and signage.

B. In addition to defining the physical limits of a facility and controlling access, a perimeter barrier also creates a physical and psychological deterrent to unauthorized entry. It delays intrusion into an area, making the possibility of detection and apprehension more likely. It aids security forces in controlling access and assists in directing the flow of persons and vehicles through designated entrances.

C. Every vulnerable point should be protected to deter or prevent unauthorized access to the facility. The roof, basement, and walls of a building may contain vulnerable points of potential entry. A security survey of the perimeter shall address manholes and tunnels, grates leading to the basement, elevator shafts, ventilation openings, skylights, and any opening 96 square inches (.061 square meters) or larger that is less than 18 feet (5.5 meters) off the ground.

D. Security and safety signage will be employed at Departmental facilities in accordance with mission needs and local municipal ordinances to serve as a notice to the public and a warning to intruders that the area is restricted and/or controlled. Multilingual signage will be used in local areas where it is customary.

E. The facility manager, in consultation with the Servicing Security Officer (SSO), determines the extent of perimeter controls based on a comprehensive security assessment. The anti-terrorism risk assessment (ATRA) should define the requirements for perimeter and other controls necessary to adequately protect the facility.

F. The assessor will evaluate the condition of general fire safety equipment including fire extinguishers, sprinklers, pull stations, smoke detectors and the fire control system. The

assessor will also evaluate the status of emergency response procedures, and the CPR and AED certification among staff members.

G. The facility manager, the SSO, and the Office of Security (OSY) Headquarters, Anti-Terrorism Division (ATD) will maintain ATRAs conducted at each Departmental facility.

30.2. FENCING

A. Fences are the most common perimeter barrier or control. Two types normally used are chain link and barbed wire. The choice depends primarily on the degree of permanence of the facility and local ordinances. A perimeter fence should be continuous, kept free of plant growth, and maintained in good condition.

1. **Chain Link.** Chain link fencing should be laid out in a straight line to permit unhampered observation. It should be constructed of No. 11 gauge or heavier wire mesh (2 inches [5.08 centimeters] square) and should be not less than 7 feet (2.13 meters) high and have a top guard. It should extend to within 2 inches (5.08 centimeters) of firm ground. It should be taut and securely fastened to rigid metal posts set in concrete. Anti-terrorism measures like surface priming may be necessary. Where a fence traverses culverts, troughs, or other openings larger than 96 square inches (.061 square meters) in area, the openings should be protected by fencing, iron grilles, or other barriers to prevent passage of intruders without impeding drainage. Chain link fencing is low in maintenance cost, a minimal safety hazard, and has openings small enough to discourage the passage of pilfered articles. A 3-foot clear buffer should be maintained on both sides of the fence. This buffer should be kept clear of anything that could interfere with a clear line of sight down the fence line.

2. **Barbed Wire.** Standard barbed wire is twisted, double-strand, No. 12 gauge wire, with four-point barbs spaced 4 inches (10.16 centimeters) apart. Barbed wire fencing, including gates intended to prevent trespassing, should be no less than 7 feet (2.13 meters) in height plus a top guard, tightly stretched, and should be firmly affixed to posts spaced not more than 6 feet (1.82 meters) apart. Distances between strands should not exceed 6 inches (15.24 centimeters).

B. Other perimeter barriers include the following devices:

1. **Concertina Wire.** Concertina wire was developed to maim people who attempt to breach a perimeter. Concertina wire will be used only in severe circumstances requiring extreme responses to localized conditions. Concertina wire will not be used to protect Departmental facilities unless approved by the Director for Security (Director).

2. **Top Guard.** A top guard is an overhang of barbed wire along the top of a fence, facing inward/outward and upward at an angle of 45 degrees. Three or four strands of barbed wire spaced 6 inches (15.24 centimeters) apart are used, but the length of the supporting arms and the number of strands can be increased when required. The

supporting arms should be affixed to the top of the fence posts and be of sufficient height to increase the overall height of the fence at least 1 foot (30.48 centimeters). Where a building of less than three stories is used to form a part of the perimeter, a top guard should be used along the outside wall to deter access to the roof.

30.3. GATES

A. A gate provides a break in a perimeter fence or wall to allow entry. Gates are secured by locks, guarded by intermittent contract guard patrols or fixed contract guard posts, protected by intrusion alarms, monitored by closed circuit television (CCTV), or by a combination of these systems. The number of gates and perimeter entrances shall be limited to those absolutely necessary. The main design consideration is to accommodate the peak flow of pedestrian and vehicular traffic.

B. Gates should be adequately lighted. Lighting requirements for gates must be coordinated with other security measures. Lighting is critical if CCTV cameras are used to monitor the gate. Gates shall be locked when not staffed and periodically inspected by a roving contract guard force. Utility openings in a fence that do not serve as gates should be locked and guarded or protected by a roving patrol.

C. Intrusion detection and access control devices may be desirable when the gate is used intermittently or when a higher level of protection is desired. Access is granted by coded cards, electronic keypads, keys, or biometric systems.

30.4. PROTECTIVE LIGHTING

Protective lighting is a valuable and inexpensive deterrent to crime. It improves visibility for checking badges and people at entrances, inspecting vehicles, preventing illegal entry, and detecting intruders both inside and outside buildings. If CCTV is employed to secure exterior or interior space, the lighting must be engineered for the application. The type of lighting (e.g., low-pressure sodium, halogen) must be selected. Environmental factors include background, pole locations, mounting, and climatology. Protective lighting should be located where it will overlap and illuminate shadowed areas and be directed at probable courses of intrusion. If justified, emergency power for lighting backup should be provided. For minimum levels, refer to the illuminating Engineering Society Lighting Handbook.

30.5. PERIMETER INTRUSION DETECTION

Protecting the perimeter of a facility that houses expensive equipment, sensitive operations, or NSI may require intrusion detection devices. Detailed guidance on intrusion detection systems and equipment that can be used for perimeter security applications can be found starting in Paragraph 30.18 to follow.

30.6. DOORS

A. Doors are prime vulnerable points in the security of any building. A door must be installed so the hinges are on the inside or protected side to preclude removal of the screws or the use of chisels or cutting devices. Pins in exterior hinges should be welded,

flanged, or otherwise secured. Hinge dowels between the hinge plates and the frame and between the hinge plates and the inside door edge should be used to preclude the door's removal. The door should be metal or solid wood. If a wooden door does not have a solid core construction or contains panels less than 1.375 inch (3.49 centimeters) thick, it should be covered on the inside with at least 16-gauge sheet steel attached with screws to provide additional protection. Life safety codes, both national and local, where applicable, must be observed. Intrusion detection systems will be employed to protect vulnerable areas if life safety concerns are present. Transoms should be sealed permanently or locked from the inside with a sturdy, sliding bolt lock or other similar device or be equipped with bars or grilles. To prevent the spread of fire, transoms should be covered with a solid sheet of wood or metal. When necessary, managers should refer to national and local fire and life safety codes to apply the appropriate standard.

B. Rolling overhead doors not controlled or locked by electric power should be protected by slide bolts on the bottom bar. Chain link doors should have a cast iron keeper and pin for securing the hand chain, and the operating shaft on a crank-operated door should be secured. A solid overhead, swinging, sliding, or accordion-type garage door should be secured with a cylinder lock or padlock and a metal slide bar, bolt, or crossbar should be provided on the inside. Metal accordion grate- or grille-type doors should have a secured metal guide track at the top and bottom and be secured with a cylinder lock or padlock.

30.7. WINDOWS

A. Windows are also vulnerable points for gaining access to a building. They should be secured on the inside using a lock, locking bolt, slide bar, or crossbar with a padlock. The window frame must be securely fastened to the building so that it cannot be pried loose. As with glass panels in a door, window glass can be broken or cut so the intruder can reach inside and release the lock. If a window is not needed for ventilation, glass block provides maximum security while permitting light to pass. Life safety codes must be observed if a window could possibly be used as an escape route. Windows that require blast resistance material are required to have acceptable retention film, or an acceptable glazing system to reduce the glass fragmentation hazard.

B. Bars or steel grilles can be used to protect a window. Bars should be at least 0.50 inches (1.27 centimeters) in diameter, round, and spaced not more than 5 inches (12.7 centimeters) apart. If a grille is used, the material should be No. 9 gauge, 2-inch (5.08-centimeter) square mesh. Outside hinges on a window should have non-removable pins. The hinge pins should be welded, flanged, or otherwise secured so they cannot be removed. Bars or grilles must be securely fastened to the window frame so they cannot be pried loose. Ensure that all operable ground floor windows are locked.

30.8. MANHOLES, GRATES, AND STORM DRAINS

Many facilities have manholes and tunnels providing service entrances into buildings. Other manholes may provide an entrance to tunnels containing pipes for heat, gas, water, and

telephone. If a tunnel penetrates the interior of a building, the manhole cover must be secured. A chain and padlock can be used to secure a manhole. Steel grates and doors flush with the ground may provide convenient access. These openings may be designed into the facility as service entrances or outside elevator entrances or they may provide light and ventilation to the basement level. If the frame is properly secured, the grates or doors can be welded into place or they can be secured with a chain and padlock. Bolting or spot welding should secure sewers or storm drains that may provide an entrance.

30.9. ROOF OPENINGS

Openings in elevators, penthouses, hatchways, or doors to roofs are often overlooked because of infrequent use. Skylights are another source of entry from roofs. These openings can be protected like windows with bars or mesh. Such protection should be installed inside the openings to make it more difficult to remove.

30.10. SHAFTS, VENTS, AND DUCTS

Ventilation shafts, vents, or ducts and openings in the building to accommodate ventilating fans or the air conditioning system can be used to enter a facility. A ventilation fan can be removed or the blade bent to make a sufficiently large opening for entry. Bars are recommended to deter such access. Screens are generally considered less desirable than bars because screens may interfere with the airflow.

30.11. FIRE ESCAPES AND BUILDING WALLS

A. Normally, outside fire escapes do not provide an entrance directly into the building; however, they can provide easy access to the roof or openings high above the ground level. Windows or other openings off the fire escape should be restricted so they can be opened only from the inside. The fire escape should be a minimum of 12 feet (3.66 meters) from the ground and/or grade.

B. Walls are not normally considered possible points of entry because of their usual solid construction; however, they cannot be disregarded because intruders may be able to break through them to gain entrance. Reinforcement at critical points may be necessary to deter forced entry.

30.12. FACILITIES IN REMOTE LOCATIONS

Large facilities located in sparsely inhabited areas have an inherent form of protection by virtue of their isolation. Constructing a fence around the perimeter usually will provide an adequate deterrent to entry. Occasional observation by a roving contract guard force may also be necessary depending on the sensitivity of the facility. CCTV systems can be especially helpful if guard forces are available to monitor them.

30.13. SIGNAGE

Warning signs or notices shall be posted to deter trespassing on Government property. Signs shall be plainly displayed and be legible, at a reasonable distance, from any approach to the

perimeter. The size and color of such signs, lettering thereon, and interval of posting must be appropriate to each situation. Refer to 41 CFR Subpart 101-20.3, Conduct on Federal Property.

A. Control Signs. Signs should be erected where necessary to assist in control of authorized entry, to deter unauthorized entry, and to preclude inadvertent entry. Bilingual signs should also be considered and are dependant on the demographics of the community. Persons in or on Departmental property shall, at all times, comply with signs of a prohibitory, regulatory, or directory nature and with the lawful direction of contract guards or other authorized individuals.

B. Other Signs.

1. **Condition of Entry.** Signs setting forth the conditions of entry to an installation or area should be plainly posted at all principal entrances and should be legible under normal conditions at a distance not less than 50 feet (15.24 meters) from the point of entry. Such signs should inform the entrant that packages, briefcases, and other containers in the immediate possession of visitors, employees, or other persons arriving on, working at, visiting, or departing from Departmental property are subject to inspection. A full search of a person and any vehicle driven or occupied by the person may accompany an arrest if necessary.
2. **Restricted Areas.** Signs or notices legibly setting forth the designation of restricted areas and conditions of entry should be plainly posted at all entrances and at other points along the perimeter as necessary.
3. **Explosives.** Signs or notices must clearly indicate that no person entering or while on Department property shall carry or possess explosives, or items intended to be used to fabricate explosives or incendiary devices, either openly or concealed, except for official purposes.
4. **Weapons Prohibited.** Section 930 of Title 18 of the U.S. Code prohibits possession of a firearm or other dangerous weapon in federal facilities, unless authorized by law, and defines "dangerous weapons" as a weapon, device, instrument, material, or substance, animate or inanimate, that is used for, or is readily capable of, causing serious bodily injury or death.

30.14. INTERIOR SECURITY CONTROLS

A. The second line of defense of the perimeter is interior controls. When an intruder is able to penetrate the perimeter controls and the building exterior, the interior controls must be able to stop further penetration. There are few facilities where every employee has access to every area in the facility. Accordingly, access to some areas will be controlled. For example, interior controls are necessary to protect NSI from unauthorized disclosure, to prevent damage to an area or to equipment, to prevent interference with operations, for safety purposes, or for a combination of these reasons.

B. Interior controls are applied to specific rooms or physical spaces within a building or facility. The facility or office manager is responsible for determining whether interior

controls are necessary. Office area controls include structural upgrades, key accountability systems, locking devices, and access control systems.

C. The extent of interior controls will be determined by considering the monetary value and mission criticality of the items or areas to be protected, the vulnerability of the facility, and cost of the security controls. Normally, the cost of security controls should not exceed the value of the item or area to be protected.

30.15. AREA DESIGNATIONS

A. **Controlled Area.** A controlled area is defined as a room, office, building, or other form of facility where access is monitored, controlled, or restricted. Admittance to a controlled area is limited to persons who have official business within the area. The senior facility manager, in consultation with the SSO, is authorized to designate an area as a controlled area after adequate security measures are in place. The following areas shall be designated as controlled areas:

1. An area where National Security Information (NSI) is handled, processed, or stored. For example, a mailroom is considered a controlled area.
2. An area that houses equipment that is valuable or critical to the continued operations or provision of services.
3. An area where uncontrolled access would interfere with or disrupt personnel assigned to the area in carrying out their official duties.
4. An area where equipment or operations constitute a potential safety hazard.
5. An area that is particularly sensitive as determined by the facility manager.
6. Law enforcement offices.

B. **Restricted Area.** A restricted area requires special constraints or controls to safeguard property or material. Admittance to a restricted area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area. Personnel without an appropriate security clearance must be escorted in a restricted area where NSI is produced, processed, or stored by personnel assigned to the area. When uncleared personnel are present in a restricted area, NSI must be protected from observation, disclosure, or removal. The facility manager, in consultation with the SSO, is authorized to designate an area as a restricted area after adequate security measures are in place. The following areas shall be designated as restricted areas:

1. Any area housing Top Secret information (see Paragraph 30.19, Security Vaults, and Paragraph 30.20, Strong rooms).
2. Any area accredited for open storage of Secret or Confidential information. This includes areas where NSI, such as charts, maps, drawings, photographs, equipment, is normally or frequently displayed, or conference rooms where NSI is being discussed. This does not include an office in which NSI is discussed or displayed and action can be taken by occupants to prevent disclosure.

3. An area used as a major repository for NSI or where NSI of substantial volume are produced or handled.
4. A telecommunications center that processes NSI.
5. An area that conducts client-server computer operations or contains highly valuable or sensitive equipment.
6. Law enforcement evidence rooms and weapons/ammunition storage areas as appropriate.
7. Any other area that is highly critical or sensitive as determined by the facility manager.

C. Working and Storage Areas for Special Access Programs.

1. **Sensitive Compartmented Information Facility (SCIF).** A protected room or office where Sensitive Compartmented Information (SCI) may be stored, used, discussed, and/or processed is called a SCIF. There are two types of SCIFs: working areas and storage areas. Prior to formal accreditation, the area must meet the rigid physical security standards set forth in the Intelligence Community Directive (ICD) 705, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities (ICS-705-1) and Standards for Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities (ICS-705-2) which supersedes Director of Central Intelligence Directive (DCID) 6/9. OSY provides liaison services with Central Intelligence Agency (CIA) on security matters and coordinates the accreditation of SCIFs within the Department.
2. **Other Special Access Program Areas.** Government agencies outside the Intelligence Community may have special access programs that require stringent physical security standards. Working and storage areas in the Department where special access program information is stored, used, discussed, or processed will be constructed in accordance with standards issued by the sponsoring agency. OSY will coordinate the approval process with the appropriate agency. To initiate the process, an operating unit head shall submit a written request with justification to OSY.
3. **Accreditation of Facilities.** SCI material can be maintained only in facilities approved by the CIA for its receipt, storage, and handling. To request establishment and accreditation of a SCIF, a request should be forwarded through the Department's Office of Executive Support to OSY. The request must include the SCI level of accreditation requested, complete address, point of contact, justification, and a description of any automated equipment that will be housed in the area.
4. Based on the request, the CIA will provide the physical security criteria for the facility to be accredited as a SCIF. Recommendations for any security upgrades will be provided to the requester. After implementing the recommendations, a

follow-up inspection will be conducted by the CIA prior to final accreditation. A final accreditation shall be provided in writing to the operating unit head, the operating unit's Security Contact, and the SSO, who will maintain a file copy in OSY.

30.16. CHALLENGE AUTHORITY

Any person within a facility, regardless of position, shall be subject to challenge by another person, the contract guard force, SSO, or any law enforcement officer, and shall display appropriate identification when challenged. Failure to do so may result in removal from the facility or other administrative action.

30.17. PROPERTY CONTROL

Facility and office managers shall establish procedures for the control and accountability of property in Departmental facilities in accordance with existing federal property regulations. The following documentation is used for property control:

A. Optional Form 7, Property Pass.

1. General Services Administration (GSA) regulations require that all property leaving federal facilities be accompanied by proof of authorized possession or ownership. The form presently in use nationwide for this purpose is the Optional Form 7, Property Pass.
2. The first step in establishing a federal property control program is to establish a cadre of officials who are authorized to sign the Optional Form 7. The list of these authorized officials must be updated periodically and should be provided to the contract guard force and to other individuals who control facility entrances. The authorized signers should be supervisors or administrative officers who are in a position to have some familiarity with the items most likely to be removed from their respective areas. They should be instructed in how to fill out the forms, how to clearly identify property, and how to maintain an accountability and follow-up program to ensure the return of federal property.
3. The contract guard force post orders at each entrance should set forth the procedures for checking outbound property, for identifying property by serial number and description, for verifying authorized signatures, and for retrieving the Optional Form 7 when the property passes their post. The contract guard force should also have instructions on how to deal with individuals who do not have the proper documentation when attempting to remove property. The contract guards should return all retrieved Optional Form 7s to the appropriate security official at least every 30 days.
4. The Security Contact should forward the retrieved Optional Form 7s to the authorized signers for follow-up action to ensure that removed federal property is properly accounted for and returned.

5. Security Contacts or facility managers may want to expedite the property control process in larger facilities by establishing a sign-in/sign-out log. Such a procedure will permit visitors to bring property into the building and leave the building the same day at the same entrance without obtaining a property pass.

B. Other Forms for Removing Property. In addition to the Optional Form 7, the following documentation may be used for removing the referenced materials from Departmental facilities:

1. CD-50, Personal Property Control. This form is used to request and account for the moving or disposal of furniture, office equipment, and other personal property from and between Departmental facilities.
2. CD-10, Publications Service Request. This form may be used to document and authorize the removal of official printed matter such as supplies of forms, pamphlets, and other Departmental-published documents.
3. Sales Receipt. A sales receipt or other documentation is used to provide proof of ownership for personally owned property.

30.18. INTRUSION DETECTION SYSTEMS

A. Purpose. Alarm systems are designed to alert security personnel or other staff of an actual or attempted intrusion into an area. These warning systems detect and report intrusions or attempts to breach a specific area. All alarm systems require a response capability to provide real protection for an area. All systems have weak points through which their effectiveness can be minimized or even completely interrupted or circumvented. Proper design and routing of cables can minimize this risk. The advantages and limitations of a variety of intrusion detection systems are described below.

B. Planning Alarm Installations. Alarms are used to detect approach or intrusion into an area. Some alarms are intended for exterior protection, and others are suitable only for indoor installations. The following criteria must be addressed in determining the need for an alarm system.

1. Sensitivity or criticality of the operation.
2. Vulnerability of the facility to damage, interruption, alteration, or other harm.
3. Sensitivity or value of the information or property stored at the facility.
4. Location of facility and accessibility to intruders.
5. Other forms of protection in place or available.
6. Response capability of the guard force or local law enforcement units.
7. Number of staff members needing access to protected areas.

C. Components of an Alarm System.

1. **Alarm Panel.** A computer inside a steel cabinet that receives signals from individual sensors and security devices. The computer can use a hard-wired system or wireless transmission to report administrative and alarm activity to monitoring stations.
2. **Alarm Sensors.** Devices that use magnetic, infrared beam, acoustical, shock, microwave, photoelectric, or moisture sensors to detect physical presence in an area.
3. **Alarm Enunciators.** A device that provides a sound and/or a visual signal to activate a system's alarm or indicate a system's malfunction. Enunciators may be combined in a system that announces alarms both locally and remotely.
4. **Emergency Electrical Backup.** A Direct Current (DC) power system that provides a supply of power to ensure continued protection in case of electrical Alternating Current (AC) power loss. Normally, enough battery capacity is provided for an emergency electrical backup system with a minimum of four hours' capacity at current load.
5. **Alarm Addressing.** A device used to identify and define zones in the security system. Typically, one or more devices may be addressed to a specific zone.

D. Alarm Annunciation. For an intrusion detection system to be effective, the alarm must annunciate, or sound, at a time and location that will generate a satisfactory response. Alarm devices use transmission lines or radio communications to relay a warning of intrusion or potential danger. Types of annunciation include the following devices:

1. **Local Alarm System.** The local alarm system has circuits within the secured area that are directly connected to audio or visual signal-producing devices such as enunciator panels, bells or sirens, or a central monitoring station located in the protected facility. Devices that do not annunciate at a panel should be mounted on the exterior of the building or, in large buildings, at interior locations where they will be audible or visible at a reasonable distance. Any alarm system should be protected against weather and tampering.
2. **Central Alarm System.** The central station receiver is connected to an alarm through telephone lines, long-range radio, cellular telephone systems, or direct wire. Central alarm systems can generate a response to a centrally located station such as a local police station or a commercial central alarm station service that provides monitoring services. When an alarm is activated, the monitoring station initiates a response either by calling personnel designated for the area or by dispatching guards to the location. Response times will vary and are based on the organizational function or the availability of response forces.

E. Types of Alarm Devices.

1. **Magnetic Contacts.**

a. Magnetic contacts consist of a magnet and a reed switch. When the magnet and the reed switch are aligned, the contact is secure. When they are not aligned, the contact is considered open. End-of-line resistors will be used to indicate whether a wire has been cut when the proper signal is not received. Magnetic switches can either be flush or surface mounted. Surface-mounted contacts are mounted on the inside of a door or opening to be protected. Flush-mounted contacts are positioned with the magnet in the area that pivots (e.g., door) and the reed switch in the stationary frame surrounding the opening.

b. Balanced magnetic contacts will be used in high-security applications. These contacts and magnets are manufactured with a matched magnet and reed switch. This ensures another magnetic field cannot be used to indicate the protected opening is secured.

2. **Passive Infrared (PIR) Devices**

a. PIR detection devices are best used in an interior environment. Wall-mounted PIR detection devices work best in a large area because the infrared beams spread with distance. Ceiling-mounted PIR detection devices should be used to provide protection in office spaces. Ceiling-mounted devices allow for movement of furniture without diminishing the coverage. Devices should be configured so that a single device provides coverage for one assigned zone. This provides a definitive location for the alarm. All PIR devices should be supervised through the use of end-of-line resistors.

b. PIR detection devices typically have a wire hole or knockout to allow the device to be wired. This hole shall be sealed with a flexible sealant such as caulk after it is wired. This will prevent insects and moisture from getting into the device.

c. PIR detection devices shall be walk-tested to ensure adequate coverage. Normally, a red light will flash in the detection device when it picks up a heat source. The heat source (e.g., human, large dog) will trigger the light within the designed range of the PIR detection device.

d. The use of ceiling-mounted PIR detection devices is highly recommended. These devices help to eliminate blind spots in coverage when offices are internally reconfigured. This is especially useful when office furniture is periodically moved.

e. **Advantages.** Infrared detection devices can be used to activate other security devices, such as cameras or microphones. PIR detection devices can also radiate beams 360 degrees.

f. **Disadvantages.** Infrared detection devices do not pick up body heat when the ambient temperature is below 38 degrees Fahrenheit.

3. **Dual Technology PIR and Microwave Sensors.**

a. Dual technology PIR and microwave sensors use two distinct technologies to provide reliable detection. Essentially, a dual technology PIR and microwave sensor will not generate an alarm unless both the PIR and microwave sensors

agree there is an intrusion. In addition, the sensors have built-in line supervision of both technologies in case of a unit failure.

b. **Advantages.** Dual technology PIR and microwave sensors are compact and easily installed, provide good coverage, are difficult to detect, have high salvage value, and are not affected by air currents, temperature, noise, light, or sound.

c. **Disadvantages.** The initial cost for dual technology PIR and microwave sensors is high.

4. **Audio Alarm Devices.**

a. Audio alarm devices use a microphone and a microprocessor to detect the breakage of glass. This detection is a two-phase event. The "thud" of the window being hit (400–600 kilohertz [kHz]) activates the microphone to detect whether the glass is actually broken (19,000 kHz). These sensors are supervised and are extremely reliable. Water is the only external influence that would degrade the performance of this type of sensor.

b. **Advantages.** Audio alarm devices have minimal installation costs, high reliability, and a 10-year life span.

c. **Disadvantages.** Line of sight must be maintained between the audio alarm device and the glass being protected. The use of heavy curtains may require installation of more sensors, which would increase the cost to properly alarm an area.

5. **Seismic Detection Devices.**

a. Seismic devices are sensitive to vibrations within the wall or structure upon which they are mounted. They have many of the same capabilities as microphones.

b. **Advantages.** Seismic detection devices are easy to install and offer effective protection for vaults.

c. **Disadvantages.** Although vibrations caused by passing vehicles or falling objects may trigger seismic detection devices, the devices can be adjusted over a period of time to compensate for false readings.

6. **Closed Circuit Television.**

a. CCTV is not primarily an alarm device but rather a monitoring device. It is frequently used as a physical security measure or as a supplement to other alarms or access control systems. CCTV systems can be used at multiple locations where visual monitoring from a remote location is advantageous, such as gates, doors, corridors, elevators, and other areas where it is not practical or cost effective to post a guard. When a CCTV system is in place, the video images shall be recorded for playback and analysis at a later time. The system shall be used in conjunction with a time/date generator that projects a continuous image of the date and time in a corner of the monitor screen. System features should include a time-lapse mode for quick playback of lengthy

periods of recorded images. Switching or multiplexing equipment must be provided in conjunction with the VCR or DVR to permit multiple screen recording and playback. When funds permit, color monitors should be considered to enhance the quality of personnel identification. The preferred countermeasure is alarm activated CCTV monitoring and recording using time-lapse video and digital image storage.

b. **Advantages.** One individual at a central station can monitor several CCTV camera locations simultaneously, and the visual image conveys much more information than other types of alarm systems.

c. **Disadvantages.** CCTV monitors do not normally provide an alarm to alert the observer, and the attention of persons monitoring television images at central stations can be distracted.

7. **Closed Circuit Television as a Detection Device.**

a. CCTV systems can be used as a detection device to trigger alarms under certain circumstances, much like space alarms where motion detection is desirable.

b. A signal generator attached to the monitor can be adjusted to project a pattern of light or dark rectangles, or windows, which can be adjusted in size and location on the screen. The windows can be focused on a fixed object to be protected or alarmed, such as a safe or a doorknob. When the image of an intruder or moving object enters the window, the difference in contrast is detected and triggers an alarm.

8. **Capacitance Alarms.**

a. A capacitance alarm is used to protect specific objects such as security containers and safes. The capacitance alarm uses the metal construction of the container and causes it to act as a capacitor or condenser. When a change occurs in the electromagnetic field surrounding the metal object, the balance is disturbed and an alarm is activated. The protective field on the container is usually maintained at a distance of not more than a few inches or centimeters from the surface of the safe. This prevents unwanted alarms activated by authorized individuals passing within a few feet or meters of the container. Very close proximity or contact with the protected object will set off the alarm.

b. **Advantages.** Capacitance alarms are compact in size, simple to install, easy to operate, and provide a high degree of security. Because they operate in an invisible protective field, capacitance alarms make it difficult to determine what is being protected. Several containers in the same area can be connected to one system.

c. **Disadvantages.** Capacitance alarms can only be applied to ungrounded equipment. In addition, accidental alarms can occur if someone touches the container.

F. **Line Supervision.** Dedicated lines that transmit the alarm signals from the protected area to the monitoring station must be protected to prevent interruption of the alarm

signal. To ensure such integrity, the transmission lines should be electronically supervised.

1. Enunciator panels are usually equipped with relays to detect changes in signal strength, although they may not be sensitive enough to detect minuscule changes. Signal line tampering can usually be detected if a low tolerance for electrical resistance is maintained in the lines. Systems with supervision tolerances less than 25 microamperes are quite effective.
2. Line supervision can be a weak link in the alarm system and should be given as much attention as other components. Accurate and complete records should be kept of all nuisance alarms.

30.19. SECURITY VAULTS

A. Purpose. A vault is a completely enclosed space with a high degree of protection against forced entry. Security vaults are commonly used for storing Top Secret information, Special Access Program information, classified communications equipment, and materials with a high dollar value.

B. Construction Criteria.

1. **Reinforced Concrete Construction.** A vault is constructed to rigid specifications. Walls, floors, and ceiling will be a minimum thickness of 8 inches (20.32 centimeters) of reinforced concrete. The concrete mixture will have a comprehensive strength rating of at least 2,500 pounds per square inch (1,133.98 kilograms). Reinforcing will be accomplished with steel reinforcing rods, a minimum of 5/8 inches (1.59 centimeters) in diameter, positioned in the concrete mixture, and spaced horizontally and vertically 6 inches (15.24 centimeters) on center; rods will be tied or welded at the intersections. Each reinforcing rod is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member.

2. **GSA-Approved Modular Vaults.** Modular vaults meeting federal specifications may be used in lieu of the above criteria. Modular vaults are flexible, movable, and expandable, and can be configured to unique space requirements. Class M vault systems accommodate Class 5 GSA-approved vault doors and are recommended by GSA for NSI and material, data, and security communication devices. The systems are accredited by the CIA for use as a SCIF.

3. **Steel-Lined Construction.** Where unique structural circumstances do not permit construction of a concrete vault, construction will be of steel alloy-type that is .25 inches (.64 centimeters) thick, having characteristics of high yield and tensile strength. The metal plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor and ceiling of reinforced concrete, they must be firmly affixed to a depth of one-half the thickness of the floor and ceiling. If the floor and/or ceiling construction is less than 6 inches (15.24 centimeters) of

reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

C. Security Vault Doors.

1. Security vault doors are categorized by their security ratings as established by GSA. All vaults shall be equipped with a GSA-approved Class 5 or Class 8 vault door (see Federal Specification AA-D-00600C). Within the United States, a Class 6 vault door is acceptable. Normally, within the United States, a vault will only have one door that serves as both entrance and exit to reduce costs.
2. Security vault door criteria are listed in the ICD 705 Technical Specifications. For further information concerning specifications and installation requirements, refer to the listed documentation.
3. Every vault door should be equipped with an emergency escape device. The escape device, not activated by the exterior locking device, should be accessible only on the inside and should be permanently attached to the inside of the door to permit escape by persons inside the vault. The device should be designed and installed so that drilling and rapping on the door from the outside will activate the escape device and thus give egress from the vault. Vault doors conforming to federal specifications will meet this requirement.
4. A decal containing emergency operating instructions should be permanently affixed on the inside of the door. Each vault should be equipped with an interior alarm or device (such as a telephone, radio, or intercom) to permit a person in a vault to contact the vault custodian or contract guard for assistance. Further, the vault should be equipped with a luminous-type light switch and, if the vault is otherwise unlighted, an emergency light.

30.20. STRONG ROOMS

A. Purpose. A strong room is an enclosed space constructed of solid building materials used to store sensitive material or high-value items in a shipping and receiving facility. Protection is normally supplemented by contract guards or alarm systems. Rooms that have false ceilings and walls constructed of fibrous materials or other modular or lightweight materials cannot qualify as a strong room.

B. Construction Standards.

1. Heavy-duty builder's hardware shall be used in construction. All screws, nuts, bolts, hasps, clamps, bars, hinges, and pins should be securely fastened to preclude surreptitious entry and to ensure visual evidence of forced entry. Hardware accessible from outside the strong room must be peened, brazed, or spot-welded to preclude removal.
2. Walls and ceilings should be made of plaster, gypsum board, metal, hardboard, wood, plywood, No. 9 gauge or heavier 2-inch (5.08 centimeter) wire mesh, or

other materials of sufficient strength or thickness to deter entry and/or give evidence of unauthorized entry. Insert-type panels should not be used.

3. Floors should be solidly constructed using concrete, ceramic tile, or wood.
4. Windows should be fitted with 0.5-inch (1.27 centimeter) horizontal bars (6 inches [5.24 centimeters] apart) and cross bars to prevent spreading. In place of bars, No. 9 gauge wire mesh can be fastened by bolts extending through the wall and secured on the inside of the window board. Windows should be kept closed and made opaque by any practical method, such as paint on both sides of the window, tempered masonite, sheet metal, or wallboard.
5. Where ducts, registers, sewers, and tunnels are of such size and shape as to permit unauthorized entry, they should be equipped with man-safe barriers such as wire mesh (No. 9 gauge, 2-inch [5.08 centimeter]) or steel bars of at least 0.5 inch (1.27 centimeter) diameter extending across their width with a maximum space of 6 inches (5.24 centimeters) between the bars. The steel bars should be securely fastened at both ends to preclude removal, with cross bars to prevent spreading. Trap doors should be dead-bolted inside the room.
6. Doors should be constructed of metal or solid wood. When doors are used in pairs, an astragal (overlapping molding) should be used where the doors meet. When the construction is of No. 9 gauge, 2-inch (5.08 centimeter) wire mesh, a similarly constructed door can be used; however, the wire mesh door should be reinforced with a metal panel at least 36 inches (.91 meters) wide, from floor to ceiling, welded to the inside of the wire-mesh wall to protect the locking device from unauthorized access or tampering.
7. Door louvers and baffle plates shall be reinforced with No. 9 gauge, 2-inch (4.08 centimeter) square wire mesh fastened to the inside of the door.
8. The doors to strong rooms shall have a computerized combination lock meeting Federal Specification FF-L-2740.
9. Depending on the value and/or sensitivity of the items contained in the strong room, consideration shall be given to the installation of a more comprehensive intrusion detection system.

30.21. FACILITIES SECURITY CHECKLIST

This checklist is furnished only as a general guide. Many of the questions will not apply to all facilities. All "YES" answers are neither a requirement nor an indication of a totally secure facility, and the reviewing SSO and/or facility manager must determine the applicability of each question to the situation at hand.

A. Perimeter/Fencing

Table 11 Perimeter/Fencing Checklist

YES	NO	QUESTION
		Is the perimeter of the facility defined by a fence or other type of physical barrier? (If possible, maintain photograph(s) or diagram(s) for exhibit purposes.)
		If a fence is used as the perimeter barrier, does it meet the minimum specifications for security fencing?
		If masonry wall is used, does it meet minimum specifications for security fencing?
		If building walls, floors, and roofs form a part of the perimeter barrier, do they provide security equivalent to that provided by the remainder of the perimeter?
		Are all openings properly secured?
		If a building forms a part of the perimeter barrier, does it present a potential means of access at the point of juncture with the perimeter fence?
		If so, is the fence height increased 100% at the point of juncture?
		Are openings, such as culverts, tunnels, manholes for sewers and utility access that permit access to the activity, properly secured?

B. Entry Points

Table 12 Entry Points Checklist

YES	NO	QUESTION
		Do the doors exceed the number required for safe and efficient operation?
		Are doors constructed of sturdy material?
		Are all entrances equipped with secure locking devices?
		Are they always locked when not in use?
		Are hinge pins to all entrance doors spot-welded or peened?
		Are all possible means of entrance to the building (e.g., ventilators, drains) covered with steel bars or adequate wire mesh?
		Are all windows securely fastened from the inside?
		Are all windows not accessible from the ground adequately secured?
		Are all openings less than 16 feet (4.88 meters) above uncontrolled ground, roof ledges, and so forth, protected by steel bars or grilles?
		Are openings less than 12 feet (3.66 meters) directly or diagonally opposite uncontrolled windows in other walls, fire escapes, roofs, and so forth, protected by steel bars or grilles?

C. Key Control

Table 13 Key Control Checklist

YES	NO	QUESTION
		Has a key control officer been appointed?
		Are locks and keys to all buildings and entrances supervised and controlled by a key control officer?
		Does the key control officer have overall authority and responsibility for issuance and replacement of locks and keys?
		Are keys issued only to authorized personnel?
		Are keys issued to personnel other than facility personnel?
		Are keys not in use secured in a locked, fireproof cabinet?
		Are records maintained indicating buildings and/or entrances for which keys are issued?
		Are records maintained indicating identification data for keys issued?
		Are records maintained indicating location and number of master keys?
		Are records maintained indicating location and number of duplicate keys?
		Are records maintained indicating issue and turn-in of keys?
		Are records maintained indicating location of locks and keys held in reserve?
		Is a current key control directive in effect?
		Are locks changed after determining lost or stolen keys will not be recovered?
		Are inventories conducted at least annually by the key control officer?
		If master keys are used, are they devoid of markings identifying them as such?
		Are employees required to report loss or theft immediately?
		Are losses or thefts of keys promptly investigated by security personnel?
		Must all requests for duplication of keys be approved by the key control officer?

D. Locks

Table 14 Locks Checklist

YES	NO	QUESTION
		Are locks on inactive gates and storage facilities under seal?
		Are they checked periodically by contract guard personnel?
		Is the manufacturer's serial number on combination locks obliterated?
		Are measures in effect to prevent the unauthorized removal of locks on open cabinets, gates, or buildings?

		Are safes located within the building?
		Are safes adequately secured to prevent removal?
		Are safes positioned to be observed from the outside by a security guard?

E. Alarms

Table 15 Alarms Checklist

YES	NO	QUESTION
		Is an alarm system used by the facility? (Give a brief description of detection device(s) on separate sheet.)
		Is it a local alarm system?
		Is it a central station system?
		Is it connected to a facility guard office?
		Is it connected directly to a monitoring station outside the facility proper?
		Is it a private protection service? Name?
		Is it a protection service provided by the local police?
		Is there any inherent weakness in the system itself?
		Is the system backed up by properly trained, alert guards?
		Is the system tested prior to activation?
		Is the alarm system inspected regularly?
		Does the system incorporate a feature to detect tampering?
		Is the system weatherproof?
		Is an alternate or independent source of power available for use on the system in the event of a power failure?
		Is the system designed to automatically switch over to the backup power source upon primary power failure?
		Is the alarm system properly maintained by trained personnel?
		Are properly screened and/or cleared personnel used in the maintenance of alarm systems?
		Are frequent tests conducted to determine the adequacy and promptness of response to alarm signals?
		Are records kept of all alarm signals received, including time, date, location, action taken, and cause of alarm?

F. Lighting

Table 16 Lightning Checklist

YES	NO	QUESTION
		Is protective lighting provided during hours of darkness?
		Is there adequate illumination for the perimeter of the facility?
		Is there an auxiliary power source?
		Are exit lights included? Stairwell lights?
		Are repairs to lights and replacement of inoperative lamps affected immediately?

30.22. IDENTIFICATION FOR ADMITTANCE TO FACILITIES

A. Forms of Authorization.

1. All forms of ID for admittance to Departmental facilities must be approved by the Director.
2. Forms of ID in an operating unit should be kept to a minimum and standardized to the fullest extent practicable to facilitate accountability and prevent unnecessary proliferation. Forms of ID should be restricted to those critical to the accomplishment of the Department's missions. Special forms of ID for unique purposes or special facilities will need justification. An example is the Census Bureau's enumerator ID for special censuses.
3. Any proposal for a new form of ID should be submitted in writing with a detailed justification through the SSO to OSY Headquarters for approval.
4. Proposals for special operating unit or facility forms of ID are covered in Paragraph 30.23, Forms of Identification.

B. Identification Possession and Display.

1. Each Departmental employee is required to possess and carry a form of employee ID while in duty status. All personnel in a facility identified as Level II - V are required to wear and display their agency photo IDs at all times when in government controlled spaces. The display of the photo ID in Level I facilities is recommended.
2. All non-employees of the Department, such as contract personnel, guest workers, research associates, and visitors, are required to possess and display personal ID. Exceptions to this policy must be approved by the SSO.
3. All Departmental forms of ID are the property of the Department.
4. No Departmental form of ID may be possessed or used unless it has been approved and issued by an authorized issuing official of the Department.

C. Authorized Use.

1. Departmental forms of ID are intended for official use only by the bearer. The forms of ID are used to identify the bearer as an employee or associate of the Department and to authorize admittance to Departmental facilities subject to local controls.
2. Departmental forms of ID are not intended for use as identification in conducting personal business. It is understood that from time to time employees will be required to identify themselves by name and photograph or by place of employment, for legitimate purposes. The Department assumes no liability for the currency or accuracy of data on the form of ID when used for such purposes.

D. Misuse. The misuse of a Departmental form of ID, including use for other than official or authorized purposes, repeated loss, failure to carry it while on duty, or refusal to show it when entering a controlled area, and so forth, may result in forfeiture of the ID and revocation of the privileges it conveys or administrative action, including discipline. Holders of Departmental forms of ID may be required to surrender the ID at any time by the issuing official or other security authority for cause. When this occurs, an escort may be required for entry into Departmental controlled space, or the individual may be subjected to the same procedures and requirements as a visitor to obtain entry.

E. Lost, Expired, and Damaged Forms of Identification.

1. The loss of any form of employee ID must be reported immediately to the issuing office, followed by a written report within three working days. The report must include a detailed explanation of the circumstances surrounding the loss.
2. The issuing officer may require a waiting period before a replacement ID is issued, to provide time for the lost ID to be recovered or for an investigation into its loss to be conducted. The Commerce Department (CD) Form 487, Visitors' Pass, should be used in the interim.
3. Each form of ID that expires or becomes unserviceable should be returned to the issuing office for a replacement.
4. Employees separating from the Department for any reason must turn in, or properly account for, their Departmental forms of ID. The processing of an employee's final paycheck may be delayed until the employee has accounted for all Government property issued to him or her, including the Departmental ID (see Department Administrative Order (DAO) 202-299).

30.23. FORMS OF IDENTIFICATION

A. Personal Identity Verification (PIV) II Credentials. This form of ID is used where the Video Imaging System is available. The vast majority of employees located in metropolitan areas or major facilities carry this form of ID. The purpose of this form is to authorize entry to Departmental facilities, subject to local procedures and restrictions, and to identify the bearer as an employee or associate of the Department. In addition, the video-imaged ID cards have a built-in electronic strip, chip, or antenna

that may replace separate key cards for entry into specified areas. Such entry may be controlled by a centralized computer system. Individuals may be given access to different areas of a facility based on their position or need for access. Facilities, with the approval of the SSO, may issue non-PIV cards to persons who will be on site less than 180 days.

B. **CD-277, Official Credential and Badge.** The Official Credential is a two-part credential, prescribed and illustrated in DAO 207-11, Official Credential and Badge. The badge is carried by authorized investigative and law enforcement personnel of the Department. Its purpose is to identify and establish the authority of the bearer, usually a Special Agent, investigator, inspector, or auditor, who performs law enforcement functions as specified in DAO 207-11. The credential is annotated to show the bearer's authority to perform enforcement duties such as conducting investigations, executing and serving search warrants, serving subpoenas and summonses, administering oaths, making arrests, making seizures of property subject to forfeiture, carrying firearms, and requiring and receiving information regarding the laws of the United States and the Department. Special Agents of certain law enforcement units of the Department are authorized to carry the Official Investigative Badge. The credential and badge shall authorize the bearer, when in the performance of official investigative or law enforcement duties, to enter any Departmental facility on a 24-hour basis without prior approval. The CD-277, Official Credential, will not be used in lieu of the issued ID card for routine access to the facility.

C. **CD-487, Temporary Visitor Pass.** The Temporary Visitor Pass authorizes visitor admittance to facilities where access is controlled and where some form of registration is required. The CD-487 may display a photograph or other personal data regarding the bearer and cannot be used for admittance during restricted hours. The pass is usually issued by a contract guard or receptionist for daytime access to a facility. When issued, it should be stamped with an expiration date not to exceed 90 days from issuance. Facilities may allow access to visitors based on existing local security policy. A formal record of these visitors must be kept at all times, either in writing or electronically.

D. **Other Forms of Commerce Identification.** Departmental operating units may develop other forms of ID for controlling access in specific facilities such as a single building or facility within a building. Use of these IDs will be limited to the specified facility or purpose and are not authorized for Department-wide use. Modifications to Departmental forms of ID will not be made without prior approval of the Director.

E. **Invalid Forms of ID.**

1. **Expired Forms.** A Departmental ID that has expired is no longer valid, does not convey the privileges it previously had, and is subject to immediate surrender. Each employee is responsible for monitoring the expiration date of his or her ID and for making timely arrangements for replacement. Expiration dates are set by the issuing authority.

2. **Obsolete Forms of ID.**

a. Forms of ID no longer in use due to a completed event or the phasing out of a unit are obsolete.
b. Any form that has been superseded by a more recent version is obsolete.

30.24. PROCEDURES FOR ISSUANCE AND RENEWAL

A. Video-Imaged Identification Card/Building Pass. An employee's supervisor may request issuance of a Departmental form of ID to the employee either through electronic means or by a memorandum to the issuing security office.

B. CD-277, Official Credential. The issuance of the CD-277 is prescribed in DAO 207-11, Official Credential and Badge.

C. Homeland Security Presidential Directive 12 (HSPD-12), dated August 27, 2004, Policy for a Common Identification Standard for Federal Employees and Contractors, directed the promulgation of a federal standard for secure and reliable forms of ID for federal employees and contractors.

30.25. ADMITTANCE TO DEPARTMENTAL FACILITIES

A. Departmental facilities house a wide variety of functions and activities that are performed by Government employees, Departmental associates, official visitors, foreign nationals, and the general public. Access to Departmental facilities during and after business hours will be controlled as specified in local security procedures.

1. Policies and procedures for access to local Departmental facilities shall be established under the purview of the ranking unit official or senior facility manager, in consultation with the SSO, and shall be in compliance with the policies and minimum standards set forth in this Manual of Security Policies and Procedures (Security Manual).

2. Decisions on admittance policy shall consider the sensitivity of the facility; the criticality of the operations; existing access controls, including contract guard forces and their response capability, and alarm systems; and the investigative process completed on the persons who will have access.

B. Basic Principles for Admission.

1. **Official.** Admittance to Departmental facilities is normally for official purposes only. In addition to employees and contractors reporting for work, official business may include inter-agency and other official calls, visits by the general public on commercial or personal business with the Department, and official functions such as meetings and ceremonies.

2. **Unofficial.** Admittance to Departmental facilities may include family visits, social functions, or other events as prescribed and approved by the facility manager or the SSO. The responsibility for the conduct of visitors rests with the sponsor or escort. Facility and security officials shall have standing procedures for carrying out such responsibilities.

3. Occasional Use of Public Buildings.
   a. Title 41 of the Code of Federal Regulations, Subpart 101-20.4, establishes rules and regulations for the occasional use of Federal Government facilities for cultural, educational, or recreational activities deemed to be in the public interest. The guidance pertains to the public areas such as auditoriums, meeting rooms, courtyards, and lobbies of buildings, and permits activities as long as they do not disrupt the operation of the building.
   b. Such use of Departmental facilities is subject to 41 CFR 101-20.4 and the regulations set forth in this Security Manual. Further information regarding this type of activity in Departmental facilities can be found in DAO 206-5, Occasional Use of Public Areas in Public Buildings, which also contains provisions for the cancellation of such events for security reasons.

C. Identification and Procedures for Admittance. A facility is normally open to the public for official business during regular business hours; however, access is restricted after business hours to protect Departmental assets. The following procedures apply to Departmental facilities where the Security Contact or the senior facility manager has instituted access controls for persons entering the facility, and a form of ID such as an ID badge with a photograph is required as an access control. Foreign nationals may be granted access to Departmental facilities or activities in accordance with DAO 207-12.

1. **Business Hours.**
   a. **Definition.** Business hours are those hours during which the facility is open for conducting official business of the Department. Certain facilities may not be open to the public, even during normal business hours, because of local restrictions. Special access controls must be observed in these facilities.
   b. **Commerce Employee Admittance.** When identification is required to gain admittance to a facility, employees will display one of the authorized Departmental forms of ID specified in Paragraph 30.23, Forms of Identification. Employees with the appropriate ID will not require escorts unless required by local restrictions or unusual circumstances.
   c. **Admittance of Maintenance and Contractor Personnel, Research Associates, Guest Workers, and Foreign Nationals.**
      1) Personnel employed by or under contractual obligation to the Department, who are required to gain access to a Departmental facility for more than 180 days, may be issued the contractor version of the Video Imaging Identification for admittance to Departmental facilities, subject to local controls.
      2) A person employed by or under contractual obligation to the Department, who is required to gain access to a Departmental facility for fewer than 180 days, shall be issued a Temporary Visitor Pass, CD-487, with an expiration date of 90 days or less assigned by the issuing official.
      3) Other foreign nationals not employed by or under contractual obligation may be admitted to Departmental facilities, provided there are sufficient

controls in place to prevent access to areas housing classified or sensitive information and restricted technology.

d. **Visitor Admittance.** Visitors may be admitted to public areas of a Departmental facility subject to local security procedures. Areas may be closed to public access when circumstances require action to ensure the orderly conduct of Government business. The decision to close public areas shall be made under GSA Federal Management Regulations or local requirements after consultation with appropriate security officials.

2. **Security Hours.**

a. **Definition.** Security hours are those hours a facility is closed to the general public when access must be limited to individuals essential to the official business of the Department. The facility manager shall institute access controls for Department facilities during security hours. Controls may include locked doors, guard posts, registration logs, and other measures to prevent unauthorized access.

b. **Admittance of Commerce Employees and Maintenance/Contractor Personnel.**

1) When forms of ID are required for admittance to Departmental facilities, employees or maintenance and contractor personnel shall display one of the authorized forms of ID specified in Paragraph 30.23, Forms of Identification, and will be subject to local restrictions prescribed by the facility manager. Some Departmental facilities may be closed to employees, contractors, and other persons as special circumstances warrant. During such special restrictions, supervisors may need to provide lists of essential persons to the facility manager or security officials to arrange for authorization to enter the facility. A completed CD-165, Admittance to Department Installations During Security Hours, other approved form, or a memorandum may be used for this purpose.

2) An employee, maintenance person, or contractor who does not have a Department-issued form of ID may enter Departmental facilities during security hours only with prior written authorization of the facility manager or SSO. The CD-165, other approved form, or a memorandum may be used for such authorization. The employee shall be bound by any established admittance procedures, such as signing a register upon entering and exiting the facility. The facility manager or security officer may require the employee to be escorted by an authorized person. Facilities may allow access to visitors based on existing local security policy. A formal record of these visitors must be kept at all times either in writing or electronically.

c. **Admittance of Research Associates, Guest Workers, Long-Term Visitors, and Foreign Nationals.**

1) Research associates, guest workers, and long-term visitors who are U.S. citizens shall obtain prior approval from a facility manager before

admittance to the facility is granted. Such access shall be subject to the processing requirements in Paragraph 11.4, Investigative Requirements for Non-Employees, of this Security Manual. Escorts are mandated for areas housing classified or sensitive information or sensitive technology. Upon admittance, the person shall register with the guard force, if any, or sign a register upon entering and exiting the facility.

2) Unrestricted access of foreign nationals or other persons who are not associated with the Department through employment or contractual obligation is not in the best interest of the Department or national security. To prevent such persons from gaining access to sensitive technology or other information without the knowledge of the hosting organization, enhanced access controls shall be instituted by the senior facility manager, Security Contact, or SSO. Foreign nationals shall be escorted at all times unless they are cleared for limited access to a specified area granted by the sponsoring official.

d. **Visitor Admittance.**

1) Departmental facilities are closed to the public after business hours. Official visitors on Government business may be admitted to facilities subject to local security procedures developed by the facility manager and the SSO. These procedures will require an escort by an authorized person while the visitor is in the facility. Visitors in the facility during business hours but remaining into security hours must be escorted by an authorized person if a facility escort requirement exists.

2) When prior approval is required for admittance, the CD-165, Admittance to DOC Installations During Security Hours, or a memorandum shall be submitted to the office overseeing physical security of the facility. An automated system with integrated authorization controls may be used as an alternative to a manual system. The facility's security procedures shall describe the routing for any necessary approvals.

3) Employees may escort family members within Departmental facilities during security hours provided such visits do not disrupt the normal business of employees. The facility manager may require a CD-165 or a memorandum for approval. The employee will be held responsible for the family's observance of all pertinent GSA and Departmental regulations while in the facility. Facilities may allow access to visitors based on existing local security policy. A formal record of these visitors must be kept at all times either in writing or electronically.

4) Requests for exceptions to the visitor admittance policy must be submitted in writing through the Security Contact to the facility manager or SSO.

5) Forms of ID shall be limited to those described in Paragraph 30.23, Forms of Identification.

D. Exceptions to Admittance Procedures. The ultimate decision to control access to a facility rests with the facility official, who shall consult with the SSO. All access control procedures shall be established in accordance with the standards prescribed in the Physical Security Criteria for Federal Facilities (see Paragraph 30.26 below). If necessary, a facility manager may strengthen the access control procedures in his or her facility. On the other hand, to accommodate unusual operations, facilities, or circumstances, local officials may prescribe less restrictive admittance procedures under the following conditions, provided they are within the guidelines established by the Physical Security Criteria for Federal Facilities (see Paragraph 30.26 below):

1. OSY must be advised in writing of the less restrictive procedures within 30 days of their implementation.
2. The senior facility manager is responsible for controlling access and monitoring the conduct of individuals who are admitted under such procedures.
3. Forms of ID shall be limited to those described in Paragraph 30.23, Forms of Identification, other Government agency forms of ID, or company or institutional identification.
4. All access control and visitor monitoring principles of this Security Manual must be observed during such operations.

30.26. FACILITY SECURITY LEVEL DETERMINATIONS FOR FEDERAL FACILITIES

Security Levels. The Department has established four security levels as a way to determine the assessment schedule for each facility within a three and five-year cycle. This complements the assessment schedule provided by the Facility Security Level (FSL) Determinations for Federal Facilities An Interagency Security Committee Standard, dated 2008. The four Department levels are as follows:

A. Departmental wholly-owned and leased Level I facilities that have 100 or fewer federal employees and less than 10,000 square feet. Other factors considered are Mission Criticality, Symbolism, Threat to Tenant Agencies, and Intangible Adjustment. Level I facilities receive a physical security risk assessment at least once every five years.

B. Departmental wholly-owned and leased Level II facilities that have 101 to 250 federal employees and 10,001 to 100,000 square feet. Other factors considered are Mission Criticality, Symbolism, Threat to Tenant Agencies, and Intangible Adjustment. Level II facilities receive a physical security risk assessment at least once every five years. At a minimum NOAA vessels (ships) are identified as Level II facilities.

C. Departmental wholly-owned and leased Level III facilities that have 251 to 750 federal employees and 100,001 to 250,000 square feet. Other factors considered are Mission Criticality, Symbolism, Threat to Tenant Agencies, and Intangible

Adjustment. Level III facilities receive a physical security risk assessment at least once every three years.

D. Departmental wholly-owned and leased Level IV facilities that have more than 750 federal employees and more than 250,000 square feet. Other factors considered are Mission Criticality, Symbolism, Threat to Tenant Agencies, and Intangible Adjustment. Level IV facilities receive a physical security risk assessment at least once every three years.

E. All facilities that house or contain designated Critical Infrastructure assets as identified by the Office of the Chief Information Officer IT Security, Infrastructure, and Technology Office receive a physical security risk assessment at least once every three years.

Note: The Department identifies its Critical Infrastructure facilities because of the criticality and national impact associated with the specific facility's mission. This designation allows OSY to place greater emphasis on the assignment and ranking of overall risk scores for all Departmental facilities.

In cases where there is an identified threat or increased risk to Departmental critical infrastructure assets, the designated official, in cooperation with OSY may assign a higher ISC FSL level of protection to adequately protect the asset.

Chapter 31. Locks and Keys

31.1. SECURITY REQUIREMENTS

The Department of Commerce (Department) aims to provide safe and secure workplaces that are open and inviting for all Departmental employees and visitors, yet maintain accountability of keys, access media, safes, and vaults. Requirements for the selection of locks to provide security for the respective working environments will depend on the assets to be protected and the local conditions. The security of any property or facility relies heavily on locking devices. Locks merely delay entry and should be supplemented with other protective devices. An assessment of all hardware, including doorframes and jambs, should be included in any physical security survey. Devices, which vary greatly in appearance as well as function and application, are described below in paragraph 31.2, Types of Devices.

31.2. TYPES OF DEVICES

A. Key Locks. Key locks are the most common locks. They include mortise cylinders, rim cylinders, padlocks, cylindrical lock-sets, tubular lock-sets and unit locks. Although a determined individual can open most key locks in a few minutes, locks are used primarily to delay and discourage or deter theft or unauthorized access.

B. Computerized Combination Locks. Computerized dialers and robotics are used to unlock mechanical combination locks. Facility managers or security contacts should refer to the General Services Administration (GSA) schedule for approved computerized combination locks and specifications.

C. Mechanical Manipulation-Resistant Combination Locks. Manipulation-resistant combination locks are no longer available through the GSA procurement system as approved combination locks. They still provide a high degree of protection, and those already in service may be used to protect classified material. Locks requiring major repairs must be replaced with a computerized combination lock meeting Federal Specification FF-L-2740. Minor repairs to the lock do not affect the storage approval of the container. Some of the more commonly used locks include the following:

1. Sargent and Greenleaf (S&G) 8400 MP locks are built-in, three-wheel combination locks. These locks can be installed on safes, security containers, vaults, and doors protecting secured areas.
2. The Mosler 302 lock is a built-in, three-wheel combination lock. It can be installed on safes, security containers, and vaults, but not on doors. Locks presently in service may remain in service until major repairs are required.

D. Key Padlocks and Combination Padlocks. Key padlocks, depending on asset and risk analysis should be high security. Characteristics of a high security padlock are: hardened shell, hardened shackle, can be shackle-less, can have a partially exposed shackle, and shackle is not held in place by a "spring" or "dog." The combination padlock is used primarily on the bar-lock filing cabinets. They are approved for storage of classified material up to and including Secret until October 1, 2012. All keys to

access controlled areas shall be inventoried at least annually. Types of padlocks currently approved for use at Departmental facilities include the following locks:

1. S&G Model 8077 is enclosed in a chromed metal shell protecting the body of the padlock. The change keyhole is located in the back of the padlock. The stated protection afforded by the exposed shackle Model 8077 is 30 man-minutes against manipulation of the lock, 30 man-minutes against radiological attack, and 10 man-minutes against surreptitious entry.
2. S&G Model 8077AB is an updated version of the Model 8077. No protection rating is available for this lock.
3. Hasp and chains used with a padlock system should provide the same level of protection as the padlock.
4. The use of grand master key locksets or universal keys should be avoided and kept to a minimum when necessary to secure Department assets.

E. Electronic and Mechanical Cipher Locks. Electronic and mechanical cipher locks are primarily used to control entry into an area. Rather than using a key, a person opens a lock by pushing a series of numbered buttons. The lock can be activated either electrically or mechanically. Examples include the Simplex Lock (mechanical) and the Continental Model S (electric). Two of the advantages of using these locks are easy combination changing and simple operation. These devices are used for access control and do not provide a high degree of security when used alone. Some models have "time penalty" and error alarm features and can be tied to an existing alarm system. When used in a controlled or restricted area that is not manned 24 hours a day, these locks must be supplemented by a built-in combination lock described above.

F. Electronic Card Key Systems.

1. An electronic access control system uses a card key programmed with a particular code read by a card reader that communicates with an automated central processor. The card reader obtains data from the card by reading bar codes, magnetic strips or spots, imbedded antennas, or any of several other methods. To open a door, the card is typically inserted into a slot, swiped through a groove, or placed in proximity to a sensor and the coded card is read by the system's reader. If the code is an authorized one, the processor will direct the lock to open.
2. Card readers fall into two basic categories: online and intelligent.
   a. Online readers must communicate with a central processor that makes the entry and exit decisions.
   b. The intelligent card reader compares the data on the card with preprogrammed data, and entry or exit is granted or denied by the card reader itself at the reader location. Intelligent readers are also called stand-alone or offline readers.
3. Multiple card readers can be used to control access to numerous buildings and rooms on one central processor. Most processors can discriminate between time

zones and levels of status for multiple readers and can record the time, date, location, and frequency of employee movements in and out of an area. Many have additional features and capabilities such as monitoring alarms, keeping time and attendance records, and communicating with emergency and law enforcement agencies.

4. Monthly personnel reports should be created by the issuing authority to identify key card holders who transfer or terminate. Supervisors are required to collect key cards or immediately notify the access control system custodian when employees or contractors transfer or terminate.

5. Key card access should be "zoned" for levels of access, and established in accordance with NIST Special Publication 800-116.

G. Biometric Systems. Other locking systems are available that use neither keys nor combinations. These systems include locks that open by identifying a fingerprint, voiceprint, or retinal image. These biometric systems are primarily designed to control access to extremely sensitive, special-use areas where positive personal identification is an operational necessity. Facility managers or Security Contacts should consult with local security professionals or contact the Office of Security for further guidance on technical specifications.

H. Homeland Security Presidential Directive 12 (HSPD-12) Compliance. Electronic and biometric access control systems must comply with HSPD-12 and NIST SP 800-116, http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

31.3. CHANGING A COMBINATION

A. When to Change a Combination. The combination to a lock must be changed in any of the following circumstances:

1. A container is placed in use.
2. An individual who knows the combination no longer requires access to the container.
3. There is reason to believe the combination has been compromised.
4. A container is taken out of service. Built-in combination locks shall be reset to the factory standard combination prior to removal from office space.

B. Selecting a Combination. When selecting combination numbers, avoid multiples of five, ascending or descending numbers, simple arithmetical series, and personal data such as birth dates and social security numbers. Use numbers that are widely separated. This can be achieved by dividing the dial into three parts and using a number from each third as one of the combination numbers. Numbers should be in high-low-high or low-high-low sequence. The same combination should not be used for more than one container in the same office. Carefully follow any manufacturer's instructions in installing combination numbers.

C. How to Change a Combination. Combination locks have either hand-change or key-change capability. Untrained individuals should not attempt to change a combination, including an XO7-9 locks (mounted combination locks); rather, they should submit lock change requests to the Servicing Security Office (SSO), locksmith, or authorized contractor.

D. Safeguarding the Combination.

1. Only those persons whose official duties require access to a security container should know its combination. The combination should be committed to memory. The combinations are to be protected at the highest classification level of material in the container. The SF-700, Security Container Information, should be filled out in its entirety and forwarded securely to the SSO. Combinations must not be carried in wallets, concealed on persons, or written anywhere other than the SF-700. SF-700s should be stored in a separate container approved for classified information up to the level of the classification of the safe.
2. When opening any kind of combination lock, personnel must ensure that no unauthorized person can learn the combination by observing the sequence of numbers being entered or dialed. It may be necessary to block the view of the dial from anyone standing nearby.

E. For more information concerning container combinations, refer to Manual of Security Policies and Procedures, Chapter 23, Storage of Classified National Security Information.

NOTE: Generic pin codes are not authorized for use in access control systems.

31.4. KEYS

A. Types of Keys.

1. **Operating or Change Keys**. Keys that employees use daily to open locks.
2. **Duplicate Keys.** Copies of change keys usually stored for use in an emergency or to replace a lost key. Duplicate keys must be kept to a minimum and protected to avoid proliferation and loss of accountability.
3. **Elicit Keys.** Keys that are illegally copies.
4. **Sub-Master Keys.** Keys that are designed to pen certain locks within a series.
5. **Master Keys.** Keys that are designed to open all locks of a particular series.
6. **Grand Master Keys.** Keys that open all locks.
7. **Master Keys.** Keys designed to open all locks of a particular series. Key systems can have one grand-master key for the overall system and several sub-master keys for each subsystem. Master keys can be used as a convenience but must be carefully controlled.

8. **Construction Keys.** Keys that open the locks installed on doors during the construction of a facility.
9. **Control Keys**. Keys used to remove the cores of locks for changing keys. These keys are used only in interchangeable core systems.
10. **Restricted Keys.** Key blanks controlled by the manufacturer and provided only to authorized issuing officials.

B. Accountability Procedures.

1. The integrity of a key system is important to safeguard property and control access to restricted areas. Lost keys minimize the effectiveness of a lock. The facility manager or SSO must provide specific guidance for maintaining the facility's key system, including storing, issuing, and accounting for all keys of a system. Keys shall be issued only to persons who have an official need. Keys not issued shall be stored in a locked container.
2. The loss of keys must be reported immediately to the issuing office followed by a written report within three working days to your SSO and senior facility officer. The report will include a detailed explanation of the circumstances surrounding the loss. Accountability records must be kept accurately, and the issuing official shall follow the instructions described below:
   a. When a key to a designated controlled or restricted area is lost, the locks to the area must be changed.
   b. Access lists for persons authorized to draw master keys shall be maintained.
   c. The key storage container shall be checked at least monthly.
   d. All keys and locks shall be inventoried at least annually.
   e. Employees should exhaust reasonable efforts to locate lost or missing keys. Replacement keys may be issued following these efforts. If the lost key is found, it must be returned immediately to the key custodian.
3. Requests for issuance of new, duplicate, or replacement keys shall be approved or monitored by the facility manager or the SSO.
4. Systems used to account for keys must include all the following information:
   a. Inventory number assigned to each key and lock.
   b. Location of each lock (room number).
   c. Name of person to whom keys have been issued.
   d. Date of issuance.
   e. Room numbers that the key will open.
   f. Signature of the recipient to whom the keys are issued.

C. Protection of Keys.

1. Office keys should be kept separate from personal keys.
2. Office keys should not be left on a desk, under a computer, or in an unlocked drawer where they can be easily taken and copied. Office keys should not be placed in a coat

and left hanging on a coat rack or draped over a chair. Office keys should be kept with a person or locked securely in a desk or cabinet.

3. An office key should not be lent to anyone.
4. If office keys are missing, personnel should immediately report the incident to the issuing officer or a member of the guard force. A security evaluation should be conducted to determine the need to re-key the office.
5. Key storage container should be UL approved (or similar) and should be mounted in a way that would delay an adversary from removing it (bolted or fastened, etc.).

Security contacts, facility managers, or other issuing officials should allow a reasonable waiting period for the replacement of lost keys. The waiting period will allow time for the lost key to be found before expending the time and expense of issuing a replacement key. Offices that issue keys should establish alternative procedures for entry by employees during the waiting period.

Chapter 32. Security Force Services

32.1. DETERMINING THE NEED

A. Introduction. The Security Force can be the cornerstone of an effective physical protection program. The effectiveness of an integrated security system of locks, barriers, lighting, cameras, intrusion detection systems, and access control systems, while critical to the success of a security posture, ultimately depends on the response by a skilled Security Force that provides the continuous state of order in the security profile, which in turn, depends on the circumstances of facility ownership and/or delegation. Security Force service(s) can be provided by various entities such as the Department of Homeland Security Federal Protective Services (DHS/FPS), a private security company under contract with DHS/FPS, a private security company under contract with the Department of Commerce (Department) for Department-owned and leased spaces, or Department-proprietary police forces.

B. Criteria for Determining Need. Security Force services are not limited to the circumstances listed below:

1. **Required.** The facility is determined to be a security level III, IV, or V according to the Facility Security Level (FSL) Determinations For Federal Facilities, an Interagency Security Committee Standard, dated April 12, 2010.

2. **Recommended.**
   a. The mission of the facility is particularly critical (e.g., a major computer facility or sensitive satellite tracking station).
   b. A high level of sensitive information is processed or stored at the facility (e.g., Classified National Security Information, sensitive technology, or economic data is processed).
   c. An in-house response capability is needed (i.e., the facility contains alarmed vaults or other sensitive operations, and off-site Security Forces or police are not close enough for quick response).
   d. The facility is vulnerable to theft or damage (e.g., a major warehouse facility or office located in a high crime area).
   e. Pedestrian or automobile traffic is heavy or congested and requires special controls.
   f. Any Department-owned or leased property where an evaluation of elevated threat profiles and risk factors determines these to be significantly reduced by the presence of a Security Force.

C. Cost Factors.

1. As with any expenditure of funds, the annual cost of Security Force services normally should not exceed the monetary value of the protected items. For example, a $50,000-per-year Security post normally would not be justified to protect $10,000 worth of furniture or to prevent the theft of $20,000 worth of non-sensitive

computers. High-value items in large quantities could clearly justify the expense of a Security Force when compensatory security measures (intrusion detection systems, high security locks, etc.) are deemed inadequate to sufficiently support the protection of the resource.

2. A substantial expense for Security Force services may be required for crowd or traffic control, for safeguarding highly classified or sensitive information, or for protecting materials or functions that have high intrinsic rather than monetary value. This is especially true when applied to the safety of employees. A Security post at the entrance to a facility that is staffed by highly qualified, trained, and professional personnel may yield substantial benefits in terms of improved safety, employee morale, increased productivity, and a better image of the Department.

D. Armed or Unarmed Security. See paragraph 32.6.N and 32.6.O for further instructions regarding armed Security and unarmed Security. The facility manager, in consultation with the Servicing Security Office (SSO), determines whether to arm the Security Forces, the number of Security posts, and hours for each post at a facility. FPS mandates that all Security Forces who operate x-ray or magnetometer equipment at General Services Administration (GSA)- owned, leased, and operated facilities must be armed. The decision should be based on a comprehensive physical security survey such as described in Chapter 29, Physical Security Program, section 29.4. The local crime rate, number of entrances, alarm systems to respond to, and other unique factors will determine the number of security posts and hours of coverage for each facility. For Departmental facilities that use contract security personnel, the bidding contractor will be responsible for calculating the total number of Security Force personnel necessary to meet the Government's minimum requirements, taking into consideration the number and duration of posts and shifts, relief requirements, sick leave, and other administrative factors. Please see the Phased Facility Security Program Handbook.

32.2. Typical Security Force Duties

Some of the duties more commonly performed by Security Forces are indicated below. Individual facility requirements will vary, and these variations should be considered in assigning security duties.

A. Entrance Control. Operate and enforce a system of access controls, including inspection of forms of identification (ID) and packages.

B. Employee/Visitor Processing and Escort Duties. Operate electronic access control systems and enforce an approved system of employee/visitor access and control. This could include escort duties to further restrict the access of visitors to a facility.

C. Roving Patrol. Patrol routes or designated areas, such as perimeters, buildings, vaults, and public areas.

D. Traffic Control. Direct traffic (vehicular and pedestrian), control parking, check permits, and issue citations.

E. **Firearms.** Carry firearms as specified and directed in the statement of work for the Security Force contract.

F. **Key Control.** Receive, issue, and account for certain keys to the facility and its internal and external areas.

G. **Security and Emergency Equipment.** Monitor and operate closed circuit television (CCTV), digital video recorders, intrusion detection systems, magnetometers, x-ray machines, explosive detection devices, etc., and respond to intrusion and fire alarm systems or use of protective and first aid devices.

H. **Utility Systems.** Monitor, record data, or perform minor operations for building utility systems.

I. **Facility Rules and Regulations.** Monitor compliance with, and enforce, posted applicable rules and regulations.

J. **Lost and Found.** Receive, store, and maintain accountability for found items.

K. **Law and Order.** Enforce local criminal statutes within the jurisdiction designated by the commissioning authority when specified in the statement of work for the Security Force contract.

L. **Hazardous Conditions.** Report all potentially hazardous conditions in accordance with the requirements of the statement of work for the Security Force contract.

M. **Response to Emergencies.** Respond to emergencies, summon assistance, obtain professional assistance in accordance with procedures in the event of injury or illness to anyone on the protected premises, and assist public safety personnel in case of any emergency such as fire, bomb threat, assault, or civil disturbance.

N. **Flying of the Flag.** Monitor flying and replacement of the United States flag.

O. **Reports and Records.** Prepare offense reports on accidents, fires, thefts, and other building incidents, including completing GSA Form 3155, Offense/Incident Report or equivalent site specific incident report form.

32.3. JURISDICTION

A. **Background.** Jurisdiction is defined, for law enforcement and protection purposes, as the legislated authority or delegation of legal authority in a defined territory, to perform law enforcement functions such as investigating criminal acts, making arrests, and prosecuting individuals for criminal violations. Jurisdiction confers legal power and all such power not delegated to the Federal Government by the U.S. Constitution is delegated to the states. The states, in turn, may delegate such power to counties and municipalities.

1. **Exclusive Jurisdiction.** Exclusive jurisdiction is power reserved to one agency for the exclusive enforcement of specific laws in a defined territory. Where the Federal Government has acquired all of the authority of the state and the state has not

reserved any of that authority, the Federal Government has exclusive jurisdiction. This power is usually confined to military reservations, airports, and other exclusively controlled federal or state installations and is not applicable to any Departmentally-owned or leased spaces.

2. **Concurrent Jurisdiction.**
   a. Two or more entities sharing powers of enforcement have concurrent jurisdiction, such as when a state or local government has delegated authorities to the Federal Government but has also retained the right to exercise those authorities itself. Most Departmental facilities, whether owned or leased, fall into this category. In the Herbert C. Hoover Building, for example, authority is shared by the DHS/FPS, which represents the Federal Government, and the Metropolitan Police Department, which represents the municipality of the District of Columbia. Another example is the United States Patent and Trademark Office in Alexandria, Virginia, where Alexandria City, with authority delegated by the State of Virginia, represents the city and DHS/FPS represents the Federal Government. There are also a limited number of jurisdictions where three entities—usually county, city, and federal—have concurrent jurisdiction.

   b. In concurrent jurisdictions, governmental units should attempt to execute a written agreement, such as a Memorandum of Understanding (MOU), to define the powers that will be shared. For example, the agency with primary (or original) authority, e.g., a county or a state, usually reserves the right to investigate and prosecute major crimes such as murder and rape. This power is often delegated to the municipal level. Lesser crimes and crimes pertaining to federal personnel and property, such as assault and theft of Federal Government property, are usually investigated by DHS/FPS.

3. **Proprietorial Interest Only.** Proprietorial interest only is the term applied to those areas wherein the Federal Government has acquired some right or title to an area in a state, district, or possession (e.g., through lease or purchase) but has not obtained any measure of the state's legislative jurisdiction over the area.

4. **Partial Areas.** Partial Areas refers to areas wherein the Federal government has been granted jurisdiction over an area in a state, certain of the state's authority, but where the state concerned has reserved to itself the right to exercise, by itself or concurrently with the United States, other authority constituting more than the right to serve civil or criminal process in the area (e.g., the right to tax private property).

   Note: If the jurisdictional status of a facility is in question, the Regional Counsel must be contacted and consulted to determine the facility status or resolve the jurisdictional issue.

B. Delegations of DHS Authority. In facilities where DHS has delegated its authority to the occupant agency, it may also delegate some or all of its enforcement powers. In many cases (such as at the Herbert C. Hoover Building), DHS may reserve certain of its investigative and prosecuting powers. When jurisdiction is delegated to an agency by the

DHS, an agreement must be negotiated with the local police to provide law enforcement responses or to continue certain necessary practices. An agency accepting DHS' delegation of authority would have to negotiate an agreement for police services. Representatives of the FPS, local police, and the Department must sign agreements of this type. Guidance and assistance for initiating a jurisdictional agreement may be obtained from the Office of Security (OSY). See also paragraph 32.5B, Facilities with DHS Delegations of Authority.

C. **Special Police Commissions.** Members of a Security Force may be granted a "Special Police" commission in some jurisdictions by state or local police. This commission allows the Security Force to exercise certain law enforcement authorities specified in the commission. If special police officers (SPO) are employed by a proprietary or contract Security Force, they must be specifically assigned the authorities stipulated by the commission and be trained and certified in accordance with the requirements of the commission. If special police officers are required as part of a contract Security Force, the contract statement of work must stipulate that need, must assign liability for the exercise of police powers by the Security Force under the contract, and must require the requisite training and certification. The jurisdiction of the Special Police commission is generally limited to the facility specified in the commission.

32.4. FEDERAL PROTECTIVE SERVICES

A. In many facilities owned, operated, or leased by GSA, the Security Force may be provided by the DHS/FPS. The FPS is a cadre of trained federal employees commissioned as special police officers whose authority is confined to federal installations, specified surrounding areas, and the routes between them.

B. FPS officials will work with security officials representing the primary tenant (agency having the greatest number of employees in a building or facility) to accommodate the security needs of the tenants.

C. Department pays DHS for the determined amount of protective services provided for the facility. In other words, the Department pays DHS a certain cost per year, per square foot of usable space, for basic protective services. The cost for additional protective services must be borne by the operating unit requesting the service.

D. FPS roving patrols respond to incidents in major cities where DHS may operate in towns without an FPS presence. Security Contacts attempting to negotiate protective assistance agreements in small cities and towns should contact their SSO for additional guidance.

E. If an operating unit requires additional FPS officers on fixed or mobile posts (e.g., in a lobby to control access or in a parking garage to control traffic), it may request such additional services from FPS on a reimbursable basis.

32.5. RESPONSIBILITY BY FACILITY TYPE

A. **GSA- Owned or Operated Facilities.**

1. In some facilities owned, operated, or leased by GSA, FPS officials may have decided to contract for security services. In such cases, a contracting officer of the appropriate GSA region will procure and maintain security services for each facility. A Contracting Officer's Representative (COR) will normally manage the contract. The COR is usually an FPS or GSA official with physical security expertise who maintains contact with the prime tenant's security officials to determine their needs and who monitors the execution of the terms of the contract for the contracting officer.
2. In many larger facilities, a representative of the primary tenant agency, an Agency Technical Representative (ATR), may work directly with DHS/FPS contracting officer and COR to develop the contract, write post orders, and monitor performance of the contract.
3. DHS/FPS contracting officials are responsible for security and suitability processing, as well as for training and certification. It is advantageous for the ATR to work closely with FPS officials, provide input as necessary, and monitor the required processing.

B. Facilities with DHS/FPS Delegations of Authority.

1. In facilities where DHS/FPS has delegated its authority to the occupant agency, it may also delegate some or all of its enforcement powers. In many cases (such as at the Herbert C. Hoover Building), DHS has reserved certain of its investigative and prosecuting powers.
2. In facilities where DHS/FPS has delegated protection authority to the agency or primary tenant, virtually all protection responsibilities are transferred to the agency, including procurement and management of security contracts.
3. Usually, DHS/FPS will retain responsibility for physical security surveys, mobile patrols, monitoring of alarms, response to incidents, requests for criminal investigations, and fire and facility safety and health inspections. DHS/FPS will provide such services at no charge to the agency beyond the protection portion of the rent. Where DHS/FPS provides COR or other specific contract security oversight functions, additional charges to the tenant agencies may accrue.
4. Under the delegation, the accepting agency is usually responsible for providing the following services:
   a. **Contracting for Security Force Services.** This is the responsibility of the facility manager, in consultation with the SSO, who should work in concert with the appropriate contracting officials. OSY will conduct the necessary suitability processing in accordance with Chapter 10, Position Designation, and Chapter 11, Investigative Processing for Suitability Determinations.
   b. **Crime Prevention Assessments and Presentations.** The operating unit may elect to have the SSO conduct these services or to contract with local security firms or law enforcement agencies.

c. **Maintenance of, and Response to, Security Systems in Place.** Local contractors are generally available to perform such maintenance and response, or DHS may be able to provide such services on a reimbursable basis in metropolitan areas.

d. **Reporting of All Serious Criminal Incidents.** All serious criminal incidents (such as murder or high-value theft) must be reported immediately through the SSO to OSY. In addition, DHS requires that all such incidents be reported to the appropriate FPS office with jurisdiction over the federal building. In Department-owned and leased facilities the local Police Department will also be notified.

5. A Department facility that has accepted DHS delegation has the option of requesting DHS to continue to provide one or more of the delegated services on a reimbursable basis.

C. Facilities with Proprietary Security Forces.

1. A proprietary Security Force consists of employees of an agency or tenant organization who have been hired exclusively for the protection of the assets and personnel of that organization.

a. **Advantages.**
   1) Loyalty to the organization.
   2) Greater incentive or motivation to perform due to usually greater compensation, benefits, and promotion potential.
   3) Lower turnover.
   4) Greater control of performance, supervision, training, staff selection, and communications.
   5) Higher morale resulting from more effective input to employee career tracks.
   6) Better law enforcement liaison.

b. **Disadvantages.**
   1) Higher salary, equipment, and overhead costs.
   2) The need for additional positions.
   3) Additional logistics and salary concerns arising from union affiliation.
   4) Recruiting problems (time lags and decreased flexibility in filling vacancies).
   5) The need for additional management resources to run the program.
   6) The possible need for SPO commissions.

c. **Processing Requirements for Proprietary Security.**
   1) Position sensitivity and suitability requirements can be found in Chapter 10, Position Designation, of this manual.
   2) Security clearance investigative requirements are specified in Chapter 11, Investigative Processing for Suitability Determinations, of this manual.

d. **Armed, Uniformed, Proprietary Personnel.**
   1) Departmental employees serving in armed security or police officer positions will carry the appropriate identification and certification when bearing firearms.

2) An officially issued firearm will be confiscated from an individual when that individual demonstrates or is suspected of apparent mental or behavioral disorders, spousal abuse, criminal activity, drug abuse, or any behavior or activity, which may, by virtue of his or her authority to carry a firearm, present an unacceptable risk or hazard to innocent parties.
3) In situations noted above, the Director for Security (Director) and Deputy Director or their representatives are authorized and responsible to confiscate an officially issued firearm and credential from any federal or contractor employee serving as an armed security or a police officer.

D. Facilities Without Proprietary Security Forces. Managers who have determined that their facilities require the establishment of a proprietary Security Force program must provide the justification for this decision to the Servicing Security Officer (SSO) and secure the approval of the Director prior to the implementation of the program.

32.6. CONTRACTING FOR SECURITY SERVICES

After deciding to contract for security services and determining the nature and extent of the required security services, the COR develops a statement of work that describes the contract effort required. If the contract is to be managed by a non-OSY COR, then OSY must be included in developing the statement of work and the review of proposals. The statement of work (SOW) should include the elements listed below.

A. COR Training Requirements. Training is determined by the level of the contract and is accomplished in accordance with Commerce Acquisition Manual 1301.670.

B. Scope of Work. A detailed description of the contract (e.g., security services, the premises, and the management and equipment required).

C. Contract Effort Required. A detailed description of productive man-hours and supervisory man-hours.

D. Services Required. All guard contracts will be performance-based contracts and monitored in coordination with OSY. The COR will oversee and monitor contract guard services through periodic on-site reviews of building-specific post orders and contract guard compliance with those orders. In addition, all contracts will be reviewed for contract compliance during the facility Anti-Terrorism Risk Assessment (ATRA), and the findings and recommendations will be recorded in the ATRA.

E. Supervision. Duties of contract manager, on-site supervisor, and key contractor personnel.

F. Authority and Jurisdiction. Permits and licenses will be established and maintained in accordance with state and local requirements for contract security.

G. Liability. The contractor is fully liable for the conduct of contract security employees and will be held accountable according to the stipulations identified within the security contract.

H. Regulations and Procedures. DHS and agency procedures for protection, including the following documentation:

1. Post Orders.
2. Conduct on Federal Property, 41 CFR Part 102-74, Subpart C.
3. Office of Federal Protective Services Policy Handbook (PBS P5930.17C), U.S. GSA, February 28, 2000.
4. Office of Management and Budget Memorandum 05-24, *Implementation of HSPD-12—Policy for a Common Identification Standard for Federal Employees and Contractors.*
5. Federal Information Processing Standard (FIPS) 201-1.
6. Federal Acquisition Regulation Sub-Part 52.2.
7. 52.204-9 Personal Identity Verification of Contractor Personnel.

I. Supplies, Materials, and Equipment.

1. Inventory of material furnished by the Federal Government, such as electrical and mechanical equipment, furniture, safes, computer and weapons cabinets, telephones, computers, and books and supplies.
2. Rules for property accountability, instructions for use of property, and requirements for safeguarding supplies, materials, and equipment.

J. Items Furnished by the Contractor.

1. Uniforms, insignia, and accessories.
2. Equipment, including flashlights, batons, belts, whistles, notebooks, and safety apparel.
3. Radios, including frequencies, permits and licenses, base stations, and detailed performance specifications for the site.
4. Firearms, including cleaning supplies, permits and licenses, holsters and ammunition, issuance and control procedures and records, storage cabinets, loading and unloading instructions and safety procedures, and training and certification requirements.

K. Qualifications of Personnel. Desirable qualities in the Security Force are developed through training and become instinctive through experience. The basic qualifications are to comprehend and comply with written and oral instructions. Security Force personnel shall be at least 21 years old, have at least a high school diploma or equivalent, and have two years of experience demonstrating the following characteristics:

1. Mature judgment.
2. Reliability and dependability.

3. Fluency in reading and speaking English.
4. U.S. citizenship.
5. Tactfulness and self-control.
6. Ability to observe, recall, and report.
7. Ability to retain composure and perform under pressure and to know when to call for assistance.
8. Ability to meet and deal effectively with the general public and with visiting dignitaries.
9. Ability to give instructions clearly, concisely, and firmly but diplomatically.
10. Good general health and physical fitness.
11. Contractors should be required to certify that their security personnel have all of the following:
    a. No physical disabilities that would hamper the performance of assigned duties.
    b. Freedom from serious illness or communicable disease.
    c. Binocular vision, correctable to 20/20.
    d. Hearing within normal speech range and volume.
    e. Unimpaired use of hands, arms, legs, and feet, and ability to run, lift, and climb stairs.
    f. Ability to wear and use all protective equipment.
    g. Mental alertness and emotional stability.

L. Suitability Requirements.

1. The contract shall contain suitability standards, instructions, forms and procedures to be followed for processing employees designated Low Risk. Unique factors such as the degree of potential for compromise or damage from misconduct could cause a severe impact on the efficiency and integrity of the service could result in higher position sensitivity. A contractor may be denied access to, or removed from, Departmental facilities when the action will protect the integrity or promote the efficiency of the federal service. In determining whether the action taken will protect the integrity or promote the efficiency of the service, appropriate consideration must be given to the basis of the specific security factors outlined in 5 CFR 731.202(b) in addition to the supplemental consideration factors provided. These standards and supplemental considerations are the basis upon which determinations of suitability are made.
2. Determinations of suitability for purposes of performing the duties described in the contract are generally decided by the Contracting Officer (CO) or COR, and should be based on an absence of the following criteria:
    a. Violations of rules and regulations.
    b. Neglect of duty.

c. Disorderly conduct.
d. Theft, vandalism, immoral conduct, or criminal activity.
e. Sale, consumption, possession, or being under the influence of drugs or intoxicants.
f. Improper use of authority or Federal Government property.
g. Weapons or safety violations.
h. Recurring tardiness or attendance problems.
i. Failure to report or take proper action on security problems.

M. Access to Classified Information.

1. Determining the Need for a Security Clearance.
   a. If contract security personnel are expected to handle or otherwise have direct access to classified information or equipment the position will require a security clearance at the appropriate level as prescribed in paragraph 32.6.M.3, below. There is no waiver from this requirement.
   b. If security personnel do not normally require access to classified information, but are incidentally exposed to classified information, such as during the discovery of an occasional violation, then no clearance is required. If security personnel encounter classified information while on duty, the security personnel will be debriefed by the SSO.
   c. If a security clearance is required, the investigative processing is described in the National Industrial Security Program Operating Manual (NISPOM) guidance; Chapter 33, Industrial Security and Chapter 12, Access to Classified National Security Information.
2. **Level of Clearance.** The level of clearance is determined by the highest classification of material handled or routinely accessed by the Security Force.
3. **Obtaining Clearances.** If a Security Force requires access to classified information, the contract must then include a completed DD Form 254, Contract Classification Specification. The facility manager coordinating the Security Force contract should check with the SSO and procurement officials regarding completion of this form. The contract must stipulate the same security processing requirements for any subcontracts.
4. **Handling Classified Information.** The contract should specify the following elements:
   a. Required security clearances and level of access required.
   b. Applicable requirements for safeguarding classified information. (A reference to Chapter 16, Classified National Security Information Policies, of this manual will satisfy this requirement). A copy of Chapter 16 from this manual should be included in the documentation provided to the contractor.
   c. The Security Force responsible for safeguarding a Departmental office, facility, or operation shall comply with all pertinent federal and Departmental regulations.

N. Armed Security. The Security Force should be armed only when there are compelling reasons. If the Security Force is armed for a deterrent effect, i.e., to prevent crime or other unauthorized activity, responsible officials must weigh the advantages and disadvantages, such as the danger to innocent personnel if a firearm is used by a member of the Security Force, the possibility of an accidental discharge, and the possibility, no matter how remote, of irrational behavior on the part of a member of the Security Force.

1. The Lautenberg Amendment to the Gun Control Act of 1968, effective September 30, 1996, makes it a felony for those convicted of misdemeanor crimes of domestic violence to ship, transport, possess, or receive firearms or ammunition. The amendment also makes it a felony to transfer a firearm or ammunition to an individual known, or reasonably believed, to have such a conviction. Government personnel and contractors are not exempt from the Lautenberg Amendment. All Departmental contracts will include language ensuring conformity with the Gun Control Act of 1968 and its amendments.
2. The facility manager, in consultation with the SSO and in accordance with the guidelines in this Manual, shall determine where and under what circumstances a contract Security Force will be armed.
3. When making a decision to arm the Security Force at a facility, the facility manager and the SSO should review the factors noted below. The CO should include requirements in the contract statement of work that will task the contractor with providing properly selected and trained personnel and maintaining appropriate performance and conduct standards based on all of the following factors:
   a. Shall be at least 21 years of age.
   b. Comprehensive firearms training, including certified annual qualification with the issued firearm, judgment shooting, and firearms safety.
   c. Knowledge of criminal law, proper use of force and lethal force response procedures in accordance with DHS and FPS policy.
   d. Judgment and emotional stability.
   e. Experience and demonstrated ability to maintain composure under pressure.
   f. A personal history free of arrests or other criminal activity.
4. The facility manager and SSO are responsible for reporting immediately to OSY any information regarding the behavior or actions of any armed member of the Security Force that might raise a question of the Security Force's compliance with the above factors. For a contract Security Force, such information will be forwarded through the COR to the SSO.
5. Security background investigative processing, with a minimum of a National Agency Check with Inquiries (NACI), is required for all members of a contract Security Force in the Department. The CO and COR must ensure that the requirements for the investigations and reinvestigations of the members of a contract Security Force required to carry firearms and weapons are specified in the contract.

6. Contractor personnel serving as an armed Security Force or as police officers in the Department may carry firearms and/or weapons in the line of duty. Departmental personnel, whether they are employees or contract security, shall carry appropriate certifications of firearms training and authority at all times while armed.
7. Contract Security Force members who are authorized, processed, trained, and certified in accordance with DHS, state, or local regulations will carry appropriate DHS, state, or local identification and certification when armed.
8. An officially issued firearm will be confiscated from an individual when that individual demonstrates or is suspected of apparent mental or behavioral disorders, spousal abuse, criminal activity, drug abuse, or any behavior or activity that may, by virtue of his or her authority to carry a firearm, present an unacceptable risk or hazard to innocent parties.
9. The confiscation of firearms from a member of a contract Security Force will be governed by the statement of work in the contract for a particular facility. The COR will monitor the process for confiscation of firearms from contract Security Force members in conjunction with the contract supervisor. The operating unit's CO shall be notified when such action is required.

O. Unarmed Security Services.

1. Once a determination has been made to have an unarmed and uniformed Security Force, the facility manager, in consultation with the SSO, and in accordance with the guidelines in this Manual, shall determine where and under what circumstances the proprietary or contract Security Force will be posted.
2. When making a decision to place an unarmed and uniformed Security Force at a facility, the facility manager and the SSO should review the factors noted below. If the Security Force is contracted, the CO should include requirements in the contract statement of work that will task the contractor with providing properly selected and trained personnel and maintaining appropriate performance and conduct standards based on all of the following factors:
   a. Minimum 21 years old.
   b. Read and speak English fluently.
   c. Judgment and emotional stability.
   d. Experience and demonstrated ability to maintain composure under pressure.
   e. A personal history free of arrests or other criminal activity.
   f. U.S. citizenship.

P. Plainclothes Security Services (If Applicable). Facility managers and SSOs may determine that certain controls are required for a facility, but that a uniformed security presence projects a more forceful image than desired. Most contractors can provide trained security personnel in civilian clothes, usually slacks and a blazer, to perform access control and reception services. This can be accomplished by adding a

requirement to the contract for the services of plainclothes security. Most jurisdictions do not allow the use of armed plainclothes security personnel.

Q. Supervisory Requirements. Supervisors must be individuals of unquestioned integrity who have demonstrated exceptional qualities of maturity and judgment with at least two years of field experience.

1. Supervision is key to effective Security Force operations whether proprietary or contract. All security contract statements of work shall specify qualifications of suitability, experience, training, and certifications to ensure the selection and assignment of suitable supervisory personnel. At a minimum, all supervisors must successfully complete supervisory or certified equivalent training in addition to basic training, and be certified in the performance of CPR and in the use of automatic external defibrillators (AED). Re-training and re-certification requirements must be met prior to their expiration. Supervisory training will be specialized and include, at a minimum, the following:
   a. Techniques for issuing written and verbal orders.
   b. Uniform clothing and grooming standards.
   c. Security post inspection procedures.
   d. Employee motivation.
   e. Relationship with agency security personnel.
2. When there will be three or more duty posts, an on-site supervisor shall be required. When there will be fewer than three duty posts, alternative means of supervision, such as a roving supervisor covering more than one site, may be considered. Regardless of the means selected, supervisory personnel shall physically visit each post at least once in each four-hour period. Supervisor(s) shall not hold the position of an on-duty Security Force member except in emergencies. In emergencies, the supervisor may staff the post for a period of time not to exceed two hours in any consecutive eight-hour period. The supervisor should maintain files containing, at a minimum, documentation of the following:
   a. Signed acknowledgement of an individual's knowledge of all Standard Operating Procedures.
   b. Conduct periodic Quality Assurance inspection reports
   c. Memoranda on policy and/or procedural changes.
   d. Employee files with all certifications, training, and disciplinary actions.

R. Training Requirements.

1. The contract should specify, in detail, training to be provided by the contractor, including the items indicated below. The contract should also include provisions for documenting all training certifications/re-certifications received.
   a. General duties, such as conduct; appearance; use of radios and equipment; non-lethal weapons such as pepper spray, tasers, batons, and handcuffs; first aid; CPR and AED, as appropriate; and emergency duties.

b. Physical protection, such as crime prevention, crime scene protection, patrol techniques, property control, and responses to alarms.
c. Enforcement, such as laws and regulations, observation and description, search and arrest techniques, and preservation of evidence.
d. Special problems, such as bomb threats and searches, hostage situations, escort duties, or civil disturbances.
e. Crimes, including criminal and civil law, vandalism, larceny, drugs and alcohol, burglary, robbery, arson, and responses to crimes in progress.
f. Firearms, including safety, policy, and procedure for use of lethal force, judgment shooting, qualification with the issued weapon, and a detailed specification of the qualifications standards to be met. The contractor is responsible for obtaining all required training and certifications.
g. Special training for supervisors, as necessary, based on unique requirements. Training for supervisors should include, at a minimum, techniques for issuing written and verbal orders, uniform and grooming standards, security post inspection procedures, and employee motivation.
h. Special requirements of the agency or facility, such as operation of access control systems, special response procedures for sensitive areas, relationship with government officials, penetration exercises, emergency evacuation plan, agency and security chain of command, and dignitary protection, may be required.
i. Refresher training, in addition to CPR/first aid/AED certifications and firearms re-certification, where applicable, should include at least 40 hours of job-related training. The results of Quality Control Inspections and client feedback will be included in this block of training for the selected subject matter.
j. Emergency readiness drills, such as evacuation, lockdown, or shelter-in-place, to ensure that personnel are aware of their responsibilities according to the facility's Occupant Emergency Plan in the event of an emergency (see Chapter 7, Emergency Planning and Evacuation).

2. Each unarmed officer will receive a minimum of 72 hours of pre-service, certified basic training covering at least the subjects listed in paragraph Q.1.a. through j. above. Armed officers will receive an additional 40 hours of pre-service training. All officers will receive a minimum of 40 certified hours of refresher training every year. Supervisors will receive a minimum of 9 hours certified, pre-service training and a minimum of 1 hour of annual refresher training.

3. To ensure that each contract security individual is properly trained and maintains qualifications in the items indicated in paragraph Q.1.a. through j. above according to DHS standards, the contractor shall provide individual security certifications and permits to the COR when requested (e.g., security certificates, handgun permits, CPR certifications). The COR shall monitor the expiration dates of the required certifications, licenses, and permits for each Security Force and shall periodically review required training to ensure that all contract security possesses the necessary

permits and authority to legally perform their duties. In cases where the DHS standards are not accessible to the contractor, Department contracting officials in consultation with OSY must develop its own training requirements that are based on DHS standards to be included as part of the solicitation for Department guard services.

S. **Reporting Work.** The contract shall specify, in detail, the procedures for recording and verifying the contractor's hours of work and a schedule of penalties or deductions for failure to properly perform the required work.

T. **Appendices to the Contract.** Appendices to the contract shall include the information listed below:

1. A summary of building or facility data, vehicle and equipment requirements, suitability and determinations, provisions for facility inspection, and a summary of productive and supervisory hours, plus a second appendix, in the form of a matrix, summarizing post hours by day, week, and month.

2. A description of each post, including all of the following information:
   a. Location and whether fixed or roving.
   b. Days, hours, and shifts of duty, including total weekly hours.
   c. Requirements for firearms, radios, and/or any other equipment.
   d. Work to be performed.
   e. Chain of command and reporting procedures.

3. A summary of Offered Hourly Rates, usually in matrix form, with blanks to fill in for each year of the contract (original plus up to four, 1-year extensions) to permit calculation of costs when the bidder submits productive and supervisory hourly rates.

4. A listing of specific metrics to measure vendor performance. Performance metrics are required for all performance-based contracts and should be developed in conjunction with servicing security and acquisition offices. The results of these measures can then be used to determine performance deductions or bonuses. Because of the broad range of typical security duties for security contracts, it is not practical to provide comprehensive guidance on performance measures; however, a limited number of examples of performance measures are provided below:

Reference cited: U.S. Department of Commerce Manual of Security Policies and Procedures, Chapter 32 (Security Force Services)

Table 17 U.S. Department of Commerce Manual of Security Policies and Procedures Checklist

YES	NO	QUESTION
		Is a copy of the Security Force contract on file for review?
		Is the COR trained in accordance with Chapter 32.6?
		Was the scope of work for the contract prepared by the COR?

YES	NO	QUESTION
		Does the contract stipulate the following:
		Scope of Work. A general description of the contract (e.g., guard services, the premises, and the management and equipment required).
		Contract Effort Required. A detailed description of productive man-hours and supervisory man-hours.
		Services Required. Basic duties of guards, by post, and work scheduling procedures (i.e., nature of coverage and duration of shift and relief assignments).
		Supervision. Duties of contract manager, on-site supervisor, and key contractor personnel.
		Authority and Jurisdiction. Contractor's permits and licenses, required weapons permits, and bonding.
		Liability. The contractor is fully liable for the conduct of his or her employees.
		Regulations and Procedures. DHS and agency procedures for protection, including the following documentation. • Officer's Duty Books. • Rules and Regulations Governing Conduct on Federal Property (41 CFR Part 102-74, Subpart C). • Federal Protective Services Uniformed Force Operations Handbook (PAS P 5930.17), U.S. GSA, July 1, 1997.
		Are the security officers equipped to perform their duties in accordance with the contract?
		Do the security officers have appropriate state licensing and/or credentials?
		Are the security officers trained to operate the facility's security equipment?
		Do the security officers have the appropriate level of clearance required for the contract?
		Are the Security Force's Standard Operating Procedures up to date?

Note: Security Officers conducting the compliance inspection will indicate the findings and corrective actions in the Anti-Terrorism Risk Assessment (ATRA)

32.7. SECURITY FORCE STANDARD OPERATING PROCEDURES

A. Security Force personnel must know what is expected of them. One of the most important elements in an effective Security Force is written Standard Operating Procedures. Procedures should be written in clear, simple language and formatted so information is easily accessible and quickly retrievable. Developed by the SSO, the COR or ATR, or a DHS contracting official, and reviewed and approved by the SSO, procedures should be reviewed by the project manager and/or the site supervisor for

suggested revisions based on the local site. The orders shall be reviewed and updated annually.

B. Standard Operating Procedures should include general orders, post orders, and special orders.

1. **General Orders.** The policies, procedures, and other basic information that apply to all posts.
2. **Post Orders.** Operational guidelines for specific posts that contain specific instructions for the security personnel to follow.
3. **Special Orders.** Short-term or limited scope instructions that cover special events of a limited duration, unusual events, or non-recurring activities.

32.8. SECURITY FORCE MANAGEMENT

A. Successful operation of a security contract requires constant and careful oversight to ensure that all aspects of the contract requirements continue to run smoothly. After initial negotiations, the COR or ATR should perform and carefully document the services listed below on a continuing basis. CORs and ATRs must have the training certifications set forth in the CAM, 1301.67, Contracting Officer's Representative Certification Program.

1. Maintain liaison with appropriate officials (e.g., FPS, SSOs, COs, and officials of the contract firm, including project managers, and other on-site officials).
2. Monitor the performance of the Security Force to ensure that post assignments are made in a timely and efficient manner; time sheets are kept accurately; property is accounted for; Post Orders are up-to-date, properly distributed, and read; and all provisions of the contract are being met.
3. Ensure that members of the Security Force have received basic training and weapons training, met any special agency or facility requirements, and are carrying the proper identification and certification of training.
4. Monitor the performance of the Security Force personnel on post, including roving patrols, to ensure compliance with Standard Operating Procedures.
5. Assess penalties for non-performance of the statement of work.
6. Ensure timely submission of all Security Force forms, reports, and other documentation required by FPS and/or the contract.

B. The Contract Security Oversight Program has been created in OSY to provide support and security-related technical assistance to COs and to CORs concerning contract security services. Questions or requests for security assistance may be directed to the Director, Anti-Terrorism Division, 1401 Constitution Avenue, NW, Washington, D.C. 20230.

Chapter 33. Storage and Destruction Equipment

33.1. Physical Protection and Storage of Materials

A. Employees or others having custody of classified or sensitive information or Federal Government property are responsible for its safeguarding and proper handling. The policy and procedures for the safe handling of such information are set forth in Chapter 22, Custody and Accountability of National Security Information, and Chapter 23, Storage of National Security Information, of this Security Manual. This chapter details the physical storage and destruction requirements for such material.

B. Many types of storage equipment are used to store classified and sensitive information, weapons, controlled substances, valuable equipment, and negotiable documents or funds. Only equipment described in this Security Manual or specifically approved by the Office of Security (OSY) may be used to store such materials.

C. To minimize the possibility of compromise of classified information, or attempts to break into and enter security storage equipment, items such as evidence, money, weapons, narcotics, and precious metals will not be stored with classified information.

D. The heads of operating units and Departmental offices are responsible for ensuring that authorized equipment is used for the protection of classified and sensitive information and property, and that employees are made aware of such requirements.

33.2. Security Containers

Security containers used to store classified information will be controlled through the Department's electronic database system, Security Manager, where possible but according to requirements outlined in Chapter 22. Each operating unit is responsible for entering information into this electronic system and for assisting the Security Contact in maintaining a record of controlled information.

A. Approved Containers. Federal specifications for security containers are developed by the Interagency Advisory Committee on Security Equipment (IACSE), which also approves equipment listed on the General Services Administration's (GSA) Federal Supply Schedule. A security container approved by GSA for storing classified information will bear a label affixed to the exterior attesting to its storage capability. Approved containers are those rated - Class 5, or Class 6 on the GSA's Federal Supply Schedule list. Older containers will normally have such an approval label affixed to the inside of the control drawer; however, the label may be missing from some containers as a result of age, damage, rehabilitation, or other modification. A missing label will require the container to be inspected and recertified by a GSA-approved inspector.

B. Types of Security Containers.

1. **Class 5** containers are not insulated for fire protection and are available in two-, four-, and five-drawer models. These containers are authorized for storage of classified material up to, and including, Top Secret in addition to weapons, cash, etc. The protection provided is:

30 minutes against surreptitious entry.
20 hours against lock manipulation.
20 hours against radiological attack.
10 minutes against forced entry.

2. **Class 6** containers afford the same protection as the Class 5; however, there is no certified forced entry protection. These containers are designed with two-, four-, or five-drawer models and are authorized for storage of classified material up to, and including, Top Secret. It provides the following protection:
   30 minutes against surreptitious entry.
   20 hours against lock manipulation.
   20 hours against radiological attack.
   No forced entry test requirement.
3. **Map and Plan Security Cabinets** are manufactured in both Class 5 and Class 6 models. The Map and Plan security cabinet can be equipped with individually locked compartments and is authorized for storage of classified material up to, and including, Top Secret.
4. **Money Safes** are Class 5 containers that come equipped with or without a channel base. For information related to the storage of funds, see Paragraph 34.3, Protection of Funds. Additional information can be obtained from the Department's Cash Management Handbook and the Department of the Treasury's Manual of Procedures and Instructions for Cashiers.
5. **Weapons Storage Containers** are Class 5 containers that come equipped with a standard seven-drawer configuration.
6. **Vaults** are used for the storage of classified information, providing they meet the construction standards specified in DCID 6/9, Physical Security Standards for SCIF. Prior to constructing or using such a facility, managers must consult with their Servicing Security Officer for certification of the vault for storage of classified information.

C. Procuring Storage Containers. Before procuring new storage containers, managers should make an effort to retire, return, declassify, or destroy unneeded classified records, files, or materials to make storage space or containers available. Managers should also check with property management personnel to determine whether surplus containers are available prior to purchasing new containers.

D. Conditionally Approved Containers.

1. For a number of years, a large number of filing cabinets with security lockbars and padlocks have been conditionally approved for classified storage up to the Secret level. Lockbar filing cabinets are easily compromised, however, and do not provide adequate protection for classified information. Therefore, these containers must be phased out of use by October 1, 2012. Until October 1, 2012, material up to the Secret level may be stored in these containers only if they are already in use. These containers must be systematically phased out and replaced with newer GSA-approved security containers.

2. Older containers manufactured by Remington Rand are approved only for the storage of information up to the Secret level. These models should be systematically phased out of service as resources permit.
   SAFETY NOTE: GSA determined that several Remington Rand cabinets, which were rated as fire retardant or fire resistant, contain asbestos that can be released into the atmosphere through normal use. Those models should be identified and given priority consideration for replacement. Managers should call their Servicing Security Officer if they have any questions about the identity of these containers.

E. Non-approved Containers. A filing cabinet is a container designed as a file storage unit with no inherent security features. There are no filing cabinets on the market that are approved by the Department for the storage of classified information.

F. Accountability of Storage Equipment.

1. The Security Contact or Servicing Security Officer must maintain a record on any vault, secure room, or container used to store classified information. The SF-700, Security Container Information, shall be used for this purpose.
2. To identify each vault or container, the Security Contact or Servicing Security Officer will externally mark each container and vault door with a number or symbol. This will aid in the accountability process and will facilitate maintenance of combinations by safe and room number.
3. Access to the combination of a vault or container used for storing classified information may be given only to those individuals who have the appropriate clearance and need to know.

G. Moving Security Containers. When security containers are moved from one location to another, even within the same building, the precautions listed below must be taken.

1. The Security Contact shall be notified of all container moves and coordinate the move with the responsible official. The Security Contact shall inform the Servicing Security Officer of the move within 24 hours of the move.
2. Security containers must be securely locked, clearly and distinctly marked to show the new destination, and accompanied by an appropriately cleared employee of the office or facility while in transit.
3. Containers of classified information must be stored within a locked or otherwise secured room. Under no circumstances should the container be left unattended.
4. The Classified Control Point (CCP) will update the –Security Manager database to reflect the new location of the security container.

H. Repairing Security Containers.

1. Persons who repair or drill security containers, vault doors, and locks must be cleared for access to the highest level of classified information stored within the container or must be escorted and continuously watched while working on the container.

2. Although repaired containers cannot be used to store Top Secret information, GSA-approved containers can be returned to their original state of security for storage up to the Secret level by meeting the following conditions:
   a. All damaged or altered parts must be replaced.
   b. When a container is drilled adjacent to or through the dial ring, the lock must be replaced with a lock meeting Federal Specification – FF-L-2740.. The drilled hole must be repaired with a tapered case-hardened steel rod (e.g., dowel, drill bit, or bearing) with a diameter and length slightly larger than the hole. When the rod is driven into the hole, a shallow recess should remain at each end of the rod that is no less than one-eighth inch or 3.175 millimeters or more than three-sixteenths inch or 4.76 millimeters deep. This will permit a substantial weld on the inside and outside surfaces. The outside of the drawer head must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts.
   c. Containers that have been drilled or repaired in a manner other than that described above cannot be restored to their original state of security integrity. The "Test Certification Label" and the "GSA Approved Security Container" label, if any, must be removed. The container must not be used for storing classified information, and a notice to that effect must be marked on the front of the container. Labels can be obtained from the OSY.

I. **Disposing of Excess or Obsolete Containers.** Before relinquishing a storage container, the Security Contact or container custodian must remove all drawers and search inside to ensure that classified material is not inadvertently left in the container. The combination must be reset to the factory setting of 50-25-50. A written statement must be placed on the container attesting that the container was checked and the combination reset.

33.3. DESTRUCTION EQUIPMENT

To properly destroy classified or sensitive material, personnel should use equipment appropriate for the type of material being destroyed. See Paragraph 22.7, Destruction of Classified Material, for further guidance regarding destruction of classified information.

Chapter 34. Shipboard and Aircraft Security

34.1. SHIPBOARD SECURITY

A. The purpose of this chapter is to provide security guidance to the National Oceanic and Atmospheric Administration (NOAA) program directors, managers, employees, and Uniform Service personnel of the NOAA Corps (NC) Officers to effectively secure Departmental vessels at sea and in port. All vessels must institute physical security programs in accordance with the security requirements contained in Chapters 29, 30, and 31 of the Manual of Security Policies and Procedures to protect life, property, and information from loss, damage, or misuse. Protective measures on vessels will include personnel and equipment under the operational or administrative control of the Department of Commerce (Department). Operating units may use this guidance to provide more stringent requirements for their own use.

B. Vessels involved in projects that require access to sensitive or Classified National Security Information (NSI) will implement appropriate safeguards to protect such information based on requirements contained in Section III, Classified National Security Information, of this Manual.

34.2. SHIPBOARD SECURITY RESPONSIBILITIES

A. The Director of NOAA's Office of Marine and Aviation Operations (OMAO) is responsible for implementing Departmental and NOAA policies as they relate to NC shipboard administrative procedures and operational activities.

B. Commanding Officers of the Marine Operating Center Atlantic and the Marine Operating Center Pacific are responsible for ensuring implementation of operational procedures and administrative policies aboard vessels of the NOAA fleet berthed, in port, or underway.

C. Servicing Security Offices (SSOs) are responsible for providing guidance, assistance, and support to NOAA for implementing security policy requirements.

D. The commanding officer of a vessel is responsible for shipboard security and will continually review, inspect, and evaluate established shipboard security measures to ensure compliance and consistency with established security policies and procedures.

E. All personnel embarked on a Departmental vessel are subject to whatever actions the commanding officer may take to ensure the safety and security of the vessel, the crew, its passengers, and cargo.

34.3. SHIPBOARD SECURITY PROGRAM

A. A ship under the administrative or operational control of the Department is considered a facility. Shipboard security programs will be established for all Department, NOAA, and NC vessels to ensure that each vessel is protected by the minimum security requirements. Such a program may consist of a qualified 24-hour gangway/security watch, a shore-based Security Force that regularly checks the ship, or a periodic

inspection procedure whereby each vessel's command may be contacted within a reasonable time frame. The nature and extent of the security program and appropriate procedures shall be established and documented by the commanding officer or a designated representative.

B. Factors that influence a shipboard security program include the following elements:

1. General Threats.
2. Specific Threats.
3. Criminal Activity.
4. Terrorism.
5. Piracy.
6. Destruction of Government Property.
7. Espionage.
8. Sabotage.
9. Weapons.

34.4. ACTIVE VESSELS

A. Commanding officers of active vessels will ensure the protection of their personnel, cargo, equipment, and property through the implementation of physical security safeguards contained in Chapters 29, 30, and 31 of this Manual and pertinent NOAA and NC directives, regulations, and orders.

B. Each vessel commander will maintain a list of key shipboard personnel and their telephone numbers for use in an emergency situation. Ship and watch officers will post this list in a convenient place for use.

C. Active vessels docked within U.S. ports shall follow security protocols in accordance with the Department of Homeland Security Director and Captain of the Port Maritime Security Levels.

34.5. INACTIVE VESSELS

A. Inactive ships may be fitted with sensors designed to detect fire, flooding, and intrusion. These sensors must be connected to alarm systems capable of ensuring that shore-based personnel are alerted for immediate response.

B. Shore-based security monitors will dispatch personnel to investigate all alarm soundings. Reports will be made of each alarm sounding and be maintained at shore-based commands.

34.6. AIRCRAFT SECURITY

A. All Departmental aircraft, their cargo and equipment, and persons under operational or administrative control of the Department shall be protected in accordance with this

chapter and Chapters 29, 30, and Chapter 31 of this Manual in order to protect life and property against espionage or sabotage, crime, attack, or misuse.

B. The purpose of this guidance is to provide security measures to Departmental personnel, NOAA Corps Officers, and NOAA program directors, managers, and employees to ensure aircraft owned or leased by the Department are safe and secure at home and abroad.

C. Operating units are required to establish security programs for all Departmental and NOAA aircraft. This Manual will be used as a basis to establish appropriate requirements as determined by respective Commanding Officers or operating unit officials.

D. Projects requiring access to sensitive information or NSI will require implementation of appropriate safeguards by the responsible officials to protect such information based on guidance contained in Section II, Personnel Security, and Section III, Classified National Security Information, of this Manual.

34.7. AIRCRAFT SECURITY RESPONSIBILITIES

A. The Director of NOAA's OMAO is responsible for implementing Departmental, NOAA, and federal regulations pertaining to aircraft administrative procedures and operational activities.

B. The Commanding Officer of the Aircraft Operations Center (AOC) is responsible for implementing security policies and procedures.

C. The SSO is responsible for providing guidance, assistance, and support for implementing security policies and procedures.

D. The senior Department employee involved in the operation or administration of an aircraft has full responsibility for aircraft security and will continuously review, inspect, and evaluate established aircraft security procedures.

E. All personnel embarked on a Departmental aircraft are subject to whatever actions the pilot may take to ensure the safety and security of the aircraft, the crew, its passengers, and cargo.

34.8. AIRCRAFT SECURITY PROGRAMS

A. An aircraft under the administrative or operational control of the Department is considered a facility. Security programs will be established for all Department and NOAA flight programs to ensure that each aircraft is protected by the minimum security requirements. The nature and extent of the security program and appropriate procedures shall be established and documented by the appropriate operational officials or their designated representatives.

B. Factors that influence an aircraft security program include, but are not limited to the following:

1. General Threats.
2. Specific Threats.
3. Criminal Activity.
4. Terrorism.
5. Destruction of Government Property.
6. Espionage.
7. Sabotage.

34.9. AIRCRAFT SECURITY

A. Commanding officers and pilots of Departmental and NOAA aircraft will implement unit, security programs, or laboratory physical security measures to protect personnel, cargo, equipment, and property while the aircraft is parked on the ground. Additionally, all pertinent NOAA and NOAA Corps directives, Federal Aviation Administration regulations, and Executive Orders will be implemented.

B. All Departmental aircraft will be secured and safeguarded as deemed necessary by the Aircraft Commander or senior official responsible for the use and operation of the aircraft. Department aircraft should be stored in an aircraft hanger if available and prudent.

When NOAA aircraft are housed on Department of Defense installations, protection should be coordinated with the host base commander. Upon coordination with the appropriate military police authority (Provost Marshal, Master-At-Arms, and Security Force Commander), the Commanding Officer and crew shall follow security protocols as required by the prevailing security detachment at the installation.

SECTION V. OTHER SECURITY ACTIVITIES AND FUNCTIONS

Chapter 35. Sensitive and Administratively Controlled Information

35.1. PURPOSE

A. The Department of Commerce (DOC) creates, receives, and maintains a wealth of "sensitive but unclassified" information that requires protection against unauthorized disclosure. Such information often concerns U.S. foreign relations, economic, technological, or scientific issues, and requires protection from access by foreign entities seeking to further their national interests or from domestic entities seeking to gain unfair advantage in business transactions. Although not classified, such information may be exempt from disclosure by statute or regulation because of its sensitivity and shall be afforded sufficient protection to safeguard it from unauthorized disclosure. Administrative controls are usually prescribed by a specific statute or federal regulation to protect sensitive information. Holders of sensitive information must become familiar with the guidance and apply all appropriate safeguards to protect such information from unauthorized disclosure. This chapter provides general guidance for the protection of sensitive information that is administratively controlled.

B. On May 9, 2008, the President signed a memorandum for heads of executive departments and agencies regarding the designation and sharing of Controlled Unclassified Information (CUI). The memorandum's purpose is to standardize practices of sharing information that does not meet the standards of security classification under Executive Order (E.O.) 13526, but is pertinent to national interests of the United States, or to entities outside the Federal Government. Further guidance on the designation of CUI will be provided by the Office of Security (OSY) as the Information Security Oversight Office lays out the framework for all Executive Branch agencies.

35.2. AUTHORITY

This chapter is issued under the authority of Department Administrative Order (DAO) 200-0, DOC Handbooks and Manuals. The provisions of this chapter comply with the applicable E.O.s, public laws, statutes, directives, and regulations issued by the Federal Government that pertain to sensitive and administratively controlled information. The following list identifies several commonly applied authorities governing the protection of sensitive information in the Department. (This list is not all inclusive.)

- Memorandum: Designation and Sharing of CUI.
- The Freedom of Information Act, as amended (5 U.S.C. § 552).
- The Privacy Act of 1974, as amended (5 U.S.C. § 552a).
- Disclosure of Government Information (15 CFR Part 4).
- Federal Information Security Management Act of 2002 (44 U.S.C. §§ 3541-3549; PL 107-347).

- Sections 9 and 214 of Title 13 of the U.S. Code, which protect from disclosure certain Bureau of the Census information.
- Invention Secrecy Act of 1951, as amended (35 U.S.C. §§ 181-188).
- The Export Administration Act of 1979, as amended (50 U.S.C. App. § 2401 et seq.).
- DOD regulations regarding the identification of records as "For Official Use Only" (FOUO) (32 CFR Part 518 Subpart D).
- Economic espionage (18 U.S.C. § 1831).
- Theft of trade secrets (18 U.S.C. § 1832).
- Disclosure of confidential information generally (18 U.S.C. § 1905).
- Utilization of federal technology (concerning transfer of technology) (15 U.S.C. § 3710).
- Unauthorized disclosure of information (26 U.S.C. § 7213).
- Prohibition on release of contractor proposals (41 U.S.C. § 253b (m)).
- E.O. 12600, Predisclosure Notification Procedures for Confidential Commercial Information, 52 Fed. Reg. 23781 (June 23, 1987).
- DAO 205-12, Public Information.
- DAO 205-14, Processing Requests under the Freedom of Information Act.

35.3. APPLICATION

Administrative controls are necessary to preclude the loss or compromise of sensitive information. Because there are many types of sensitive information in the Department, subcategories of sensitive information are not identified in this chapter. Each head of an operating unit or Departmental office is responsible for developing and implementing in writing additional administrative controls, as required, to protect sensitive information in his or her respective unit or office. For guidance on the administrative controls required to protect sensitive information not covered in this Security Manual, individuals should consult the originator of the material to determine what protective measures are required.

35.4. ROLES AND RESPONSIBILITIES

A. The Director for Security (Director) shall perform the following:

1. Issue Departmental policies, procedures, and guidance necessary to protect and safeguard sensitive unclassified and administratively controlled information.
2. Assist the heads of operating units or Departmental offices to implement the provisions of this chapter.
3. Assist the heads of operating units to coordinate the protection of sensitive information involving more than one department or agency, as necessary.

B. Heads of operating units or Departmental offices shall perform the following:

1. Implement the provisions of this Security Manual to protect and safeguard sensitive and administratively controlled information.
2. Issue additional policies, procedures, and guidance, as necessary, to protect and safeguard sensitive and administratively controlled information in their respective organizations.

3. Ensure that employees in their respective organizations receive the training necessary to protect and safeguard sensitive and administratively controlled information.

C. The Office of the Chief Information Officer (OCIO) shall be responsible for the following:

1. Issuing policies, procedures, and guidance for the accreditation of sensitive information technology (IT) systems used in processing and electronically transmitting sensitive information.
2. Coordinating with the OSY, Counterespionage Division (CED), in reporting security violations or infractions involving unauthorized disclosure of sensitive and administratively controlled information.

D. Servicing Security Officers (SSOs) shall perform the following:

1. Assist their operating unit in the application of the procedures of this chapter.
2. Assist their operating unit with periodic evaluations of the categories of sensitive information generated by their organization and in the application of any additional protective measures that apply to this information.
3. Provide guidance and awareness materials to employees on the proper handling of sensitive information.

E. Employees shall be responsible for the following:

1. Protecting sensitive or administratively controlled information in their possession and returning such information to the appropriate Departmental office prior to terminating employment or association with the Department or when the information is no longer needed in the performance of assigned duties.
2. Becoming familiar with, and adhering to, guidance provided in this Security Manual to protect sensitive information.
3. Ensuring they are knowledgeable of applicable statutes, policies, procedures, or regulations issued by an operating unit or Departmental office in order to protect sensitive information.

35.5. "FOR OFFICIAL USE ONLY" INFORMATION

A. Use of For Official Use Only in the DOC.

1. Information that has not been given a security classification pursuant to the criteria of an E.O., but which may be withheld from the public because disclosure would cause harm to an interest protected by one or more Freedom of Information Act (FOIA) exemptions, shall be considered as being For Official Use Only (FOUO). Information not expressly protected by a statute shall not be designated FOUO. In addition, FOUO is not authorized as a less stringent form of classification to protect national security interests that are not classified. Examples of statutes that exempt sensitive information from disclosure to the public include the Export Administration Act, the Invention Secrecy Act, Title 13 of the U.S. Code concerning

census information, Title 18 of the U.S. Code concerning Trade Secrets, and the Freedom of Information Act (FOIA).

2. The FOUO designation may be applied by any secretarial officer, head of an operating unit, senior Departmental official, or program manager who processes, handles, or maintains information that may be withheld from public disclosure under appropriate laws. The FOUO designation may also be applied to other information that has been determined by a DOC official to be sensitive (e.g., national economic policy not yet publicly released, pending reorganization plans, or sensitive travel itineraries).
3. The prior application of FOUO markings is not a conclusive basis for withholding a record that is requested under the FOIA. When such a record is requested, the information in it shall be evaluated to determine whether there is a sound legal basis for withholding the record under one or more FOIA exemptions. For specific determinations regarding the application of the FOIA to sensitive information, contact the Department's FOIA Officer. Assistance concerning the application of FOIA laws may also be obtained from the relevant operating unit's FOIA Officer or from the Department's Office of the Assistant General Counsel for Administration.
4. In order for specific information to be identified as FOUO, the following criteria must be met:
   a. **Category Test.** Information under consideration for identification as FOUO information must satisfy both of the following requirements:
      1) Unclassified (i.e., not Restricted Data (RD), Formerly Restricted Data (FRD), or National Security Information (NSI).
      2) Exempt from public release based on the FOIA.
   b. **Sensitivity Test.** Information under consideration for identification as FOUO must, in the judgment of the originator, be information that satisfies both of the following requirements:
      1) There is a legitimate Government interest in restricting disclosure.
      2) Protection of the information from disclosure outweighs the public's right to know this information.

B. Designating FOUO Information. This designation applies to unclassified information that may be exempt from mandatory release to the public under the FOIA. The FOIA specifies nine exemptions which may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. They are:

1. Information which is currently and properly classified.
2. Information that pertains solely to the internal rules and practices of the agency. (This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)

3. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.

4. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness.

5. Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.

6. Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

7. Records or information compiled for law enforcement purposes that (a) could reasonably be expected to interfere with law enforcement proceedings; (b) would deprive a person of a right to a fair trial or impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others, (d) disclose the identity of a confidential source, (e) disclose investigative techniques and procedures, or (f) could reasonably be expected to endanger the life or physical safety of any individual.

8. Certain records of agencies responsible for supervision of financial institutions.

9. Geological and geophysical information concerning wells.

C. Marking FOUO Information.

1. A document containing unclassified, sensitive information shall be marked FOUO on the bottom of the front cover (if any), on each interior page that contains FOUO information, and on the outside of the back cover (if any). Each paragraph containing FOUO information shall be marked as such. Exceptions to this policy may occur only if specific guidelines are used to protect the sensitive information such as census information protected under Title 13 of the U.S. Code from unauthorized disclosure. In all cases, the recipients of FOUO information shall be made aware of the status of such information and that special handling requirements may apply (see Paragraph 35.6B. below).
2. Operating units may wish to identify a record as FOUO at the time of creation to provide notice of FOUO content and thereby facilitate review when a record is requested under the FOIA. Records requested under the FOIA that do not bear such markings shall not be assumed to be releasable without examination for the presence

of information that requires continued protection and qualifies as exempt from public release.

3. When a document contains both classified and FOUO information, the classified markings shall be applied at the top and bottom of each page with the highest security classification of information appearing on each page (see Chapter 19, Marking). An individual page that contains FOUO information but no classified information shall be marked FOUO at the top and bottom of the page. Individual paragraphs shall be marked at the appropriate classification level as well as unclassified or FOUO, as appropriate.
4. To ensure the FOUO information will be protected after a classified document has been declassified, the following annotation should be made in the lower right-hand corner of the document:

   This document becomes "FOUO" upon declassification.
5. FOUO material transmitted outside the DOC may require the application of an expanded marking to explain the significance of the FOUO marking. This can be accomplished by typing or stamping the following statement on the record prior to transfer:

   Example:
   This document contains information exempt
   from mandatory disclosure under the [list reference]
   Exemption(s) _____ apply.
   Determined by: _____ Date: _____
6. FOUO information transmitted by electronic or facsimile media shall be clearly marked before the beginning of the text and, if necessary, throughout the text to identify the part of the message that is FOUO.

D. Transmitting FOUO Information.

1. FOUO information may be disseminated within DOC operating units and Departmental offices to conduct official business of the Department. Recipients shall be made aware of the status of such information, and transmission shall be by means that preclude unauthorized public disclosure. Transmittal documents shall call attention to the presence of FOUO attachments or enclosures. Within a DOC facility, the Form CD-494, Sensitive Information Cover Sheet, shall be used to cover FOUO documents transmitted between offices.
2. DOC holders of FOUO information are authorized to convey such information to officials in other Departments or agencies of the Executive and Judicial branches to fulfill a governmental function, except to the extent prohibited by the Privacy Act. Records thus transmitted shall be marked FOUO, and the recipient shall be advised that the information may qualify for exemption from public disclosure based on a FOIA exemption or other appropriate statute or regulation and that special handling instructions may apply.

3. Transmittal documents containing FOUO information require special markings to call attention to the presence of FOUO attachments or enclosures and shall be transported in a manner that prevents unauthorized disclosure of the contents.
4. Before sending FOUO information outside an office or the Department, all such documents shall be enclosed in a single, opaque envelope or wrapping. The envelope shall not bear any FOUO markings. If additional protection is required, senders may also opt to double-wrap the material, plainly marking both sides of the inner envelope with the marking, FOUO. Both envelopes shall be fully addressed to the appropriate official by name and title. The outer envelope shall not bear any FOUO markings. When not commingled with classified information, FOUO material may be sent via first-class mail or parcel post, although, when practicable, a courier is the preferred method for local delivery.
5. For release of FOUO information to the Legislative Branch, officials should consult the Office of Legislative Liaison for the Department or the legislative liaison for the operating unit.
6. Electronic transmission of FOUO information is authorized for the conduct of official business. Methods of electronic transmission include voice discussions over a public telephone line, sending documents to or from a non-secure facsimile (fax) machine, or data transmission using a non-secure computer network (i.e., e-mail). FOUO information should be encrypted in transmission because there is no expectation of protection of information sent over an unprotected network; however, a strict prohibition of such transmittal could seriously restrict the efficient operation of an operating unit or office. DOC officials must realize that non-encrypted transmissions may be monitored, intercepted, and modified. The following guidelines must be followed when transmitting FOUO information through non-secure electronic systems:
   a. FOUO information may be transmitted electronically if the originator of the information does not prohibit the transfer of the FOUO information by such means. If necessary, the sender will consult with the originator of the information to determine whether it is permissible to transmit the information electronically through an unprotected network.
   b. FOUO information normally should not be discussed over the telephone or transmitted electronically through an unprotected computer network unless the risk of loss or compromise of that information has been evaluated and the sender has determined the benefit of sending the information outweighs the risk of its loss or compromise.
   c. FOUO information may be transmitted over a non-secure facsimile (fax) machine without encryption; however, it is incumbent upon the sender to verify the fax number to which the material is being sent. Verification of the number requires the sender to contact the office by telephone and verify the correctness of the fax number. In addition, arrangements must be made for an authorized person to stand by the fax machine and promptly receive the transmission, thus precluding unauthorized disclosure or dissemination.

d. The sender must verify the identification of the recipient's phone/fax number or e-mail/Internet Protocol (IP) address before sending the information or calling the individual. The sender should not leave FOUO information in an individual's voicemail box.
e. If the information reveals vulnerabilities or information that could potentially cause damage to the originator, sender, or receiver if lost or compromised, the sender must evaluate the risk of transmitting the information through an unprotected network and proceed only upon concluding that the benefit of transmission exceeds potential loss or compromise.

7. Because requirements for the security of unclassified, sensitive information vary for different applications, organizations should identify their information resources and determine the sensitivity to and the potential impact of losses to confidentiality, integrity, and availability of such information. The overall security level for a particular information system must be chosen to provide an acceptable level of security for the given application and environment in which the system is used. Technical requirements for specific levels of security can be obtained from current standards in the Federal Information Processing Standards (FIPS) series of publications issued by the National Institution of Standards and Technology (NIST) and NIST Special Publications for Information Security.

E. Safeguarding and Storing FOUO Material.

1. During normal working hours, FOUO information must be stored in an out-of-sight location to ensure visitors and other unauthorized persons cannot obtain access to it. FOUO information must not be left unattended.
2. During non-duty hours, FOUO material shall be stored to prevent unauthorized access. Such material may be stored with other unclassified material in unlocked filing cabinets, desks, or bookcases when normal Federal Government or Government-contractor internal building security measures are adequate during non-duty hours (e.g., guard force, restricted access, etc.). When internal security measures are not available or when office spaces can be accessed after hours by authorized but unescorted personnel who do not have a need to know (e.g., custodial staff, maintenance personnel, etc.), FOUO materials shall be stored in a locked room, filing cabinet, or other appropriate container.

F. Destruction of FOUO Material.

1. The originator of FOUO information or other competent authority shall be held responsible for the continued review and prompt removal of FOUO markings when the information no longer requires protection from public disclosure. When FOUO status is terminated, all known holders shall be notified, to the extent practicable. Upon notification, holders of such information in the Department shall efface or remove the FOUO markings, but records in files or storage do not need to be retrieved solely for that purpose.

2. FOUO material shall be destroyed by any means that prevents the disclosure of its contents. Burning is not required for the destruction of FOUO material, unless specified by instruction of the originator. Non-record copies of FOUO materials may be destroyed by tearing each copy into pieces to prevent reconstructing the information and placing the strips in regular trash receptacles. When local circumstances or experience indicates that this destruction method is not sufficiently protective of FOUO information, local authorities may direct other methods for destroying the information; however, due consideration must be given to the additional expense balanced against the degree of sensitivity of the FOUO information contained in the records. Crosscut shredders (used for destruction of classified material) may be used for this purpose.
3. Records copies of FOUO documents shall be disposed in accordance with the instructions provided by the Department's Records Control Officer or by the records control schedule of a particular operating unit or Departmental office.

G. Reproduction of FOUO Information. FOUO information may be reproduced without obtaining specific approval of the originator, unless otherwise noted on the document. Copies must be marked and protected in the same manner as the original. Copy machine malfunctions must be cleared, with all paper paths checked for any remaining material.

H. Mishandling, Loss, or Unauthorized Disclosure of FOUO Material.

1. The unauthorized disclosure of FOUO information does not constitute an unauthorized disclosure of DOC information classified for security purposes. Appropriate administrative action shall be taken, however, to determine responsibility for the unauthorized disclosure whenever feasible, and appropriate disciplinary action shall be taken against those persons responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act or other specific statute may also result in civil and criminal sanctions against responsible persons.
2. Any person who has knowledge or suspects a violation or infraction involving the mishandling, loss, or unauthorized disclosure of FOUO information shall do one or both of the following:
   a. Take custody of the information, if necessary, and safeguard it in an appropriate manner.
   b. Promptly notify his or her Security Contact or SSO that there has been an unauthorized disclosure of FOUO information.
3. The Security Contact shall ensure that the originator of the information and the SSO are notified and action is taken to prevent further occurrence.

I. Denial and Appeal for Release of FOUO Information.

1. Several of the operating units generate, process, handle, or store sensitive information that falls under the FOUO designation above. Each head of an operating unit or Departmental office shall be responsible for providing guidance to individuals in his or her respective organizations for protecting sensitive

information. Each employee shall ensure that sensitive information is afforded the appropriate level of protection and is not released to the public if protected by a FOIA exemption or other statute.

2. When FOUO information is requested for release to the public, the information shall be evaluated to determine whether there is a sound legal basis for withholding the information under one or more FOIA exemptions or another statute. Any reasonably segregable portion of a record shall be provided to the requester after deletion of the exempted or protected portions. The amount of information deleted shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by a FOIA exemption or other statute or regulation under which the deletion is made. If technically feasible, the amount of information deleted shall be indicated at the place in the record where such deletion is made.
3. Throughout the DOC, selected officials have been delegated the authority to initially deny requests for records in the respective units for which they are responsible. The list of such denial officials is provided in 15 CFR, Part 4, Appendix B, Officials Authorized to Deny Requests for Records Under the Freedom of Information Act, and Requests for Records and Requests for Correction or Amendment Under the Privacy Act.
4. When an initial request for a record has been denied in whole or in part, or has not been timely determined, or when a requester has received an adverse initial determination under the Department's FOIA regulations, the requester may file a written appeal, which must be received by the Assistant General Counsel for Administration within 30 calendar days after the date of the written determination or, if there has been no determination, on the last day of the applicable time limit (see 15 CFR 4.10).

35.6. PROTECTION OF OTHER SENSITIVE INFORMATION

A. Departmental offices and operating units that generate or maintain sensitive information must protect such information in accordance with federal laws, regulations, or operating-unit-specific policy. In addition, several DOC operating units have a memorandum of understanding (MOU) with other agencies regarding the protection of specific types of sensitive information. For specific policies and procedures protecting such sensitive information or if a conflict arises in reference to an MOU or other agreement, personnel should consult with the operating unit or Departmental office originating the information to clarify applicable policies and procedures. Such information may require a greater level of protection than that required for FOUO information.

B. The authority, handling, storage, safeguards, and disposal for information in the following categories are described in the Department's or the respective operating unit's guidance for that specific information. Questions concerning proper use and protection of such information should be made to the appropriate DOC office that maintains and oversees that information. For example, questions concerning the protection of procurement information should be referred to the Office of Acquisition Management;

questions concerning protection of official personnel information should be referred to the Office of Human Resources Management.

1. **Procurement Information.** Departmental procurement information, including proprietary information, contract proposals, and source selection information, shall be protected from unauthorized disclosure as specified in the Commerce Acquisition Regulation (CAR) and Federal Acquisition Regulation (FAR). Individuals who handle this information in the course of their official duties shall review the relevant sections of the CAR and FAR to become familiar with the requirements for handling sensitive procurement information.
2. **Personally Identifiable Information (PII).** PII includes, but is not limited to, leave records, social security information, reports of investigations, employee addresses and telephone numbers, benefit information, medical records, performance appraisal data, financial information, and records of disciplinary actions. Information relating to personnel or personnel management in the possession or control of the Department may be required to be withheld from disclosure under the Privacy Act. The FOIA may also exempt such information from public disclosure. Additional guidance on handling and transmission of PII may be obtained from the Director, Office of Human Resources Management, a servicing human resources management office or the OCIO.
3. **Travel Information.** Travel itineraries and related documents may be sensitive and may require handling and safeguarding in some circumstances. An example would be travel information that, if disclosed, might jeopardize the physical safety of Departmental personnel, facilities, or their dependents as well as U.S. citizens overseas when there is an assessed terrorist threat to the person traveling on official business or a general threat to U.S. citizens present at locations to be visited. In most cases, travel-related information is no longer sensitive when travel has been completed.
4. **Personnel Investigative Information.** Personnel security files, background investigations, credit reports, and other investigative records shall be safeguarded based on guidance in the Department's Privacy Act Systems of Records. Personal information in such records and files also will be subject to protection from unauthorized release by the FOIA.
5. **FOIA Exemptions.** Other information held by DOC personnel that is subject to the FOIA shall be protected from unauthorized disclosure.

35.7. IT Security-Related Material

The OCIO has determined that information that contains detailed technical information about the security of an IT system, its security requirements, and/or the controls planned, recommended, or implemented requires protection from unauthorized disclosure. Sensitive IT security-related information shall be marked FOUO to provide protection against unauthorized disclosure. This information includes, but is not limited to, the system security plan, risk analysis, contingency and disaster recovery plans, certification and accreditation testing and results, internal control

reviews, and verification reviews. Other guidance for protection of IT information can be found in the Office of the CIO's *IT Security Manual.*

35.8. FOREIGN RELATIONS AND FOREIGN AFFAIRS INFORMATION

Unless classified for national security reasons, the following information received from other departments or agencies is sensitive and should be handled and safeguarded as FOUO information:

A. Information that, if improperly released, could have a negative impact on foreign policy or relations, including negotiations between governments, private businesses, international financial and monetary institutions, or official representatives, including deliberative process documents and attorney-client communications.

B. Information considered critical to the Department's foreign affairs mission, including policy or positions for bilateral or multilateral negotiations, consultations, or international agreements.

C. Information in connection with trade agreements, anti-dumping, and countervailing duty cases.

35.9. "SENSITIVE BUT UNCLASSIFIED" INFORMATION

Sensitive But Unclassified Information, (SBU) is a Department of State term. It is information that is not classified for national security reasons but that warrants/requires administrative control and protection from public or other unauthorized disclosure for other reasons. SBU should meet one or more of the criteria for exemption from public disclosure under the FOIA (which also exempts information, protected under other statutes), 5 U.S.C. 552, or should be protected by the Privacy Act, 5 U.S.C. 552a.

35.10. "LIMITED OFFICIAL USE" INFORMATION

"Limited Official Use" (LOU) is a designation used by the Department of State and its bureaus. The term is generally equivalent to the Department's FOUO. Such information should be protected accordingly. The office originating the LOU information should be contacted for any safeguarding and dissemination requirements.

Chapter 36. Mission Critical Threats to the Department

36.1. PURPOSE

This chapter provides general guidance for Departmental personnel, Servicing Security Offices (SSOs), and Security Contacts concerning the Department of Commerce (Department) policy and activities for identifying, assessing, and/or managing mission critical security threats.

36.2. AUTHORITY

Under Department Organization Order (DOO) 20-6, the Director for Security (Director) shall advise and represent the Assistant Secretary on policies and procedures for assessing any threat to the mission, operations, or activities of the Department, and provide guidance and assistance to Departmental offices and operating units on the protection of personnel, assets (including facilities, property, and classified and sensitive information), and activities. Furthermore, the Director will provide security services when it is more practical or economical to consolidate them at the Department level, and may re-delegate authorities to designated personnel in the office.

A. The Director's authorities in the following areas are delegated to qualified Office of Security (OSY) Investigations & Intelligence Division (IID) staff:

1. Conduct investigations under the authorities, functions, and responsibilities of OSY.
2. Provide services in the functional area of identification, assessment, and management of threats.
3. Ensure effective support of the National Intelligence Program by identification, assessment, and management of mission critical threats, including support of National Security Decision Directive 189 (National Policy on the Transfer of Scientific, Technical and Engineering Information) with respect to Departmental research activities, and Presidential Decision Directive 12 (Security Awareness and Reporting of Foreign Contacts) with respect to Departmental personnel.
4. Ensure effective implementation of National Security Decision Directive 298 (National Operations Security), for matters involving the identification, assessment, or management of mission critical threats.
5. Serve as the Department's liaison with agencies of federal, state, and local government in security, protection, and Departmental counterintelligence issues for matters involving the identification, assessment, and management of mission critical threats, or whenever IID staff directly act to protect Departmental personnel, facilities, property, assets, and activities from mission critical threats.
6. Provide services in the functional area of emergency actions and preparedness, including intelligence and protective services with respect to critical incidents and national continuity events.

7. Obtain special deputation from the United States Marshals Service, or otherwise by law, for the authorization to carry firearms and make arrests in order to carry out the protective functions assigned to the Director and certain members of OSY for executing IID functions.

B. As necessary, IID staff may exercise other authorities delegated by the Director or permitted by law or regulation, in furtherance of the identification, assessment, and management of mission critical threats or other IID responsibilities.

36.3. MISSION CRITICAL THREATS

A. Mission Critical Threat. A mission critical threat is a person, entity, or circumstance that creates a security concern by having the actual or constructive intent and capability to interfere in an unlawful or dangerous manner with the Department's mission, or otherwise jeopardize, compromise, or adversely exploit Departmental personnel, assets, or activities, including any such action that would either have a significant impact on the Department's ability to execute its mission or otherwise affect a greater United States Government interest.

B. Threat Spectrum. Threats to the Department's mission include those posed by influential criminal activity; foreign intelligence & security services and non-state actors; terrorism; and extremist groups or unstable persons. Threats also include significant events that may require the Department to take emergency action, such as geopolitical crises, natural disasters, and pandemics.

36.4. INVESTIGATIVE FUNCTIONS

A. Proactive Identification, Assessment, and Threat Management. When possible, OSY's goal is to prevent or mitigate the occurrence of a mission critical threat. Pursuant to DOO 20-6 and Department Administrative Order (DAO) 207-11, Department Special Agents employed by OSY's Investigations & Intelligence Programs are duly appointed Federal law enforcement officers authorized to conduct investigations. IID Special Agents will employ the full range of investigative techniques permitted by law or regulation to identify and/or assess unreported or unrecognized threats to the Department's mission, operations or activities, including examining any initiative, project, program, process, function, or incident involving the Department. IID Special Agents will also commence or coordinate investigations and operations to protect Departmental personnel, assets, and activities from recognized mission critical threats.

1. **Assistance from Departmental Personnel.** Departmental personnel are required to promptly and fully provide IID Special Agents any relevant information or necessary assistance within the scope of their employment that may aid in the prevention or mitigation of a mission critical threat.

   a. **Use of Nondisclosure Agreements.** IID Special Agents may administer nondisclosure agreements in which persons, including Departmental personnel, consent to provide confidentiality in the interests of national security, or to preserve evidence.

b. **Review of Departmental Records.** IID Special Agents may review Departmental records relevant to identifying and/or assessing a mission critical threat, confirming or dispelling suspicions or allegations during investigations, conducting damage assessments, or facilitating a threat management operation.

2. **Exemption from Departmental Requirements.** Unless prohibited by law, IID Special Agents are exempt from compliance with Departmental substantive and procedural requirements when such compliance would significantly interfere with executing the provisions of Section 36.4 as related to investigations. Serious disputes arising from this exemption may be resolved by the Secretary or Deputy Secretary.

3. **Investigative Coordination.** Criminal violations of law may be referred to the Departmental OIG as required by DAO 207-10, or an appropriate investigative or criminal justice agency with jurisdiction.

B. Other Investigative Activities. Upon request from the Secretary, Deputy Secretary, Chief Financial Officer (CFO)/Assistant Secretary for Administration, or Director, IID Special Agents may conduct security-related due diligence inquiries or other investigative activities as permitted by law or regulation.

36.5. INTELLIGENCE FUNCTIONS

A. Threat Reporting and Analysis. OSY will produce a Strategic Threat Briefing to account for recognized mission critical threats specific to the Department and Tactical Intelligence Overviews to monitor reporting relevant to Departmental security interests. In addition to conducting investigations described in Section 36.4 to support these products, IID staff will obtain and analyze all-source information, both internal and external to the Department. IID staff may also produce other threat-related information collection & analysis projects, assessments, products, reports, or briefings upon request from the Director, or in accordance with IID authorities, functions and responsibilities.

1. **Gatekeeper Initiative.** IID staff may exercise authority delegated by the Director to disseminate reporting to Departmental personnel, when such dissemination is subject to appropriate vetting, complies with applicable laws and regulations, would enhance the successful completion of an IID responsibility, and is reasonably expected to reduce the Department's security risk.

2. **Preparation of Classified or Controlled Material.** As needed, IID staff will prepare materials relevant to IID functions and responsibilities for original classification by the Director under authority delegated by the Secretary. IID staff may independently designate material as derivatively classified (pursuant to E.O. 13526), Controlled Unclassified Information (CUI), Law Enforcement Sensitive Information (LES), or Originator-Controlled Information (ORCON).

3. **LES and ORCON Disclosure Penalties.** Departmental personnel who disseminate LES or ORCON information provided by IID staff without authorization from the Director are subject to disciplinary action under DAO 202-751 as a security regulation violation.

B. Emergency Management. IID staff provide intelligence support to OSY's Continuity and Emergency Preparedness Division. During continuity events or emergency incidents, IID staff may disseminate raw, unevaluated intelligence information to key decision-makers and operating unit components when such information presents a high risk or high consequence to the Department.

Scope and Assistance. IID Special Agents engaged in emergency management intelligence support are authorized to enter or traverse through emergency or disaster areas, and may access any Departmental facility. IID Special Agents may also provide emergency dignitary and/or force protection security services to protect Departmental personnel, assets, and activities as needed.

36.6. COLLABORATION

A. Proactive Collaboration or Assistance to Other Departmental or Governmental Elements with a Nexus or Benefit to Departmental Security. IID Special Agents may initiate, participate in, or be detailed to Intelligence or Law Enforcement Community working groups, task forces, platforms, projects, or assignments involving criminal intelligence, protective intelligence, counterintelligence, counterespionage, or counterterrorism matters with a nexus or benefit to Departmental security, including U.S. Government-wide initiatives, providing assistance to other U.S. Government agencies, and operations with a federal interest that occur at the state or local level. Collaboration with other government elements outside of the United States is subject to approval by the U.S. Department of State, U.S. Department of Justice, or U.S. Department of Defense, as applicable.

B. Monitoring Conversations. IID Special Agents shall perform for the Director all liaison activities with external agencies approved by the Secretary under DAO 207-9.

C. Special Assistance to Other Departmental or Governmental Elements. Upon written request of the head of a Departmental or other governmental element and with approval from the Secretary, Deputy Secretary, CFO/Assistant Secretary for Administration, or Director, IID staff may furnish assistance to other Departmental or governmental elements, when OSY has charter authority under DOO 20-6 to meet such requests, complies with applicable laws or regulations, and the request is favorably reviewed by the Office of General Counsel.

36.7. POLICY SUPPORT

A. U.S. Government-wide Strategies. IID staff will serve as principal representative of the Department in matters regarding national strategies that address mission critical threats, and shall provide recommendations to the Director pertaining to the impact and integration of such strategies.

B. Departmental Security Policies. IID serves as principal advisor to the Director regarding mission critical threats. IID staff will evaluate and/or recommend policies and procedures related to DOO 20-6 authorities, functions and responsibilities, or present recommendations to the Director regarding exceptions to this chapter's provisions.

C. **OSY Special Agent and Investigator Programs.** IID staff will administer OSY's Special Agent and Investigator Programs, perform compliance inspections, and recommend to the Director organization, authorized activities and standards of service for all OSY employees designated as U.S. DOC Special Agents or Investigators.

Administrative Misconduct Inquiries. IID staff will receive full access to information produced during administrative misconduct inquiries involving OSY Special Agents or Investigators, particularly whenever such inquiries are initiated, make significant progress, or are closed. IID Special Agents will independently conduct administrative misconduct inquiries involving suspicions or allegations against any OSY employee involving improper use or representation of Federal law enforcement authority. Investigations confirming reportable misconduct will be forwarded to the Departmental OIG pursuant to DAO 207-10 and other applicable governmental agencies as necessary.

36.8. APPLICATION

A. **Coverage.** This chapter applies to all Departmental organizations and personnel, including full-time, part-time, and temporary employees; contractors; experts and consultants; guest workers and research associates; foreign national visitors and guests; interns and volunteers; and any other person who works directly on Departmental activities, projects or programs, referred to collectively as "Departmental personnel."

B. **Policy, Implementation, and Compliance.** The Director promulgates all Departmental policy pertaining to this chapter. All operating units will develop internal procedures implementing this chapter's requirements, subject to review, approval, and compliance inspections by IID staff.

Exceptions. When consistent with law and regulation, requests for exceptions to this chapter's provisions require written authorization from the Director.

C. **Delegation.** On a limited basis, IID staff may delegate certain functions described in this chapter to qualified Departmental personnel when approved by the Director and not inconsistent with law or regulation.

36.9. PERSONNEL RESPONSIBILITIES

Personnel (including OSY Employees, SSOs, Security Contacts, and Emergency Operations Center (EOC) Watch/Duty Officers):

A. **Awareness.** SSOs and Security Contacts are responsible for ensuring that all Departmental personnel (except for foreign national visitors and guests) receive appropriate threat information when provided by IID staff.

B. **Threat Reporting.** Departmental personnel are responsible for following the procedures outlined in Chapter 6 (Incident Reporting) to report any knowledge of mission critical threats. If Departmental personnel are unable to implement those procedures, they shall report directly to IID staff, with IID staff providing necessary information to the EOC and the appropriate Servicing Security Office or Security Contact.

1. **Coordination.** Except for imminent threats to life or property, Departmental personnel will not report matters involving mission critical threats to any other governmental entity outside of OSY without approval from IID staff or permission from the Director.
2. **Sensitivity.** Information regarding threats posed by foreign intelligence security services will be reported to IID staff either in person or via secure means.
3. **Disposition.** IID staff will examine reported information and make a determination to retain the issue for IID action or will advise the EOC Watch/Duty Officer, Servicing Security Office, or Security Contact to refer the matter to an appropriate governmental entity for disposition. EOC Watch/Duty Officers, SSOs, and Security Contacts will provide IID staff with additional or updated information upon request.

C. Additional Reporting. Departmental personnel will inform their Servicing Security Office or Security Contact in a timely manner about any Departmental activity of which they believe is especially sensitive, innovative, or mission critical, including but not limited to key infrastructure, technology development, intergovernmental collaborative projects, or international treaty development.

D. Other Government Agency Involvement. Information requested, assistance offered, or action taken by other governmental agencies pertaining to mission critical threats will be promptly reported by all Departmental personnel (including OSY employees, EOC Watch/Duty Officers, SSOs, and Security Contacts) to IID staff for review, coordination, and/or approval. Departmental personnel requested by other government agencies to execute nondisclosure agreements involving mission critical threats will decline and direct the agency's representative to contact IID staff for official coordination.

Chapter 37. Industrial Security

37.1. PURPOSE

This chapter sets forth the industrial security policies and procedures for Department of Commerce (DOC) participation in the National Industrial Security Program (NISP) for contracts, purchase orders, awards, and grants, where performance by contractors, consultants, grantees, or advisory committee members require access to National Security Information (NSI). For ease of understanding, all these individuals are called "contractors" in this chapter. The chapter assigns responsibilities for program implementation and supplements the National Industrial Security Program Operations Manual (NISPOM) guidance for the DOC.

37.2. APPLICABILITY

The provisions of this chapter apply to all DOC Departmental offices, bureaus, operating units, and field organizations that use the services of contractors who must obtain access to NSI and/or Special Access Program (SAP) contracts.

37.3. AUTHORITY

The NISP was created to provide a uniform program of baseline security requirements and standards to which all agencies, departments and contractors would adhere and against which they would be measured. Through the NISP, the Department of Defense (DoD) extends access to NSI to DOC contractors and federal advisory committee members who have appropriate security clearances.

37.4. REFERENCES

A. Executive Order (E.O.) 12829, National Industrial Security Program, January 6, 1993, as amended by E.O. 12885, dated December 14, 1993.

B. E.O. 13526, Classified NSI, December 29, 2009.

C. E.O. 12968, Access to Classified Information, August 7, 1995.

D. E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor, Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008-

E. DoD Manual 5220.22-M, National Industrial Security Program, January 1995, as amended July 1997 and February 2001.

F. Federal Acquisition Regulation (FAR) Part 4, Subpart 4.4, Safeguarding Classified Information within Industry.

G. Atomic Energy Act of 1954, as amended (Public Law 83-703).

H. Intelligence Community Directive (ICD) 704, Personnel Security Standards and Procedures Governing Eligibility and Access to Sensitive Compartmented Information and Other Controlled Access Program Information".-.

37.5. POLICY

All classified information entrusted to contractors in connection with Departmental programs and projects shall be effectively safeguarded in accordance with existing laws, applicable E.O.s, and the provision of the DoD NISP.

Participation in the NISP allows DOC to use the Defense Security Service (DSS) to conduct investigations for contractor facility and personnel clearances and to monitor the contractor's compliance with safeguarding requirements. There is no charge to DOC for these services. In order to activate DSS services and obligate the contractor to the provisions of the NISPOM, a DD Form 254, "Contract Security Classification Specification", must be included in all classified contracts and contract solicitations.

37.6. DETERMINATION OF FACILITY CLEARANCE AND PERSONNEL CLEARANCE OF CONTRACTORS

A. Verification of Facility Security Clearance (FCL). Prior to the disclosure of any classified information to a contractor, the responsible Contacting Officer Representative (COR) must obtain verification that the contractor's facility is in possession of a valid FCL equal to or higher than the level of classified information to be disclosed in the performance of the contract. Requests for verification shall be submitted in writing to the Office of Security (OSY), Counterespionage Division (CED) from either the Security Contact or Servicing Security Officer (SSO), on the DD 254 form, and contain all of the following information:

1. Name and location of the contractor facility.
2. Brief description of the work to be performed.
3. Level of access to classified information required.
4. A statement of whether or not the facility is to receive, generate, use, and/or store classified information in the performance of the contract.
5. The estimated volume of classified information segregated by classification level, to be provided to, and/or generated by, the contractor.
6. The name and telephone number of the point of contact at the contractor facility who is knowledgeable and responsible for the contract.
7. The name, telephone number, and e-mail address of the contractor's Facility Security Officer.

B. Verification of Personnel Security Clearance (PCL). OSY/CED shall provide security clearance verification for DOC contractors. Proof of contractor's PCL may be provided to OSY/CED by the Security Contact or SSO. Requests for verification of a contractor's PCL shall be submitted on the DD 254 from the Security Contact or SSO and contain the following information:

1. Name of Contractor.
2. Date of Birth.
3. Place of Birth.

4. Social Security Number.

37.7. RESPONSIBILITIES

A. OSY/ CED shall perform the following functions:

1. Furnish assistance and guidance to contracting and program personnel relating to the security requirements of any procurement action involving classified or sensitive information.
2. Furnish assistance and guidance to committee control officers relating to processing requests for security clearances for members of federal advisory committees (see Chapter 11, Investigative Processing) and facility security clearances under the NISP.
3. Receive requests for and verify facility security clearances for prospective contractors or employers of advisory committee members.
4. Process and grant security clearances for designated independent contractors and/or consultants (see Chapter 11, Investigative Processing).
5. Assist the contractor, contracting officer, or program official, in the development of security classification guidance for contractors requiring access to classified information.
6. Represent the Department in all NISP matters with other federal departments, boards, committees, and so forth.

B. Contracting officers shall be responsible for ensuring that appropriate and specific security classification guidance is issued for all classified contracts. Security classification guidance is prepared by the program official in coordination with the OSY/CED. The contracting officer shall perform the following functions:

1. Coordinate with the COR and the Security Contact to ensure protection of classified information in the possession of contractors and pertaining to contracts.
2. Ensures the statement of work outlines specific duties relating to the need for accessing classified information in their association with the DOC, and specific language is included stating, "Contractor agrees to comply with the NISPOM."
3. Obtain verification from OSY/CED of a facility and personnel security clearance through the Security Contact and/or the SSO prior to the disclosure or release of any classified information to a contractor.
4. Review and approve the Contract Security Classification Specification, DD Form 254, including taking the following actions:
   a. Submit all DD Form 254s to the Defense Security Service (DSS) at:
      Defense Security Service
      2780 Airport Drive, Suite 400
      Columbus, Ohio 43219-2268
   b. Issue a DD Form 254 (revised) whenever a modification to the contract occurs and/or classified duties and needs change during the course of the classified contract. Provide a copy of the revised DD Form 254 to the Security Contact or SSO.

c. Review, in coordination with the responsible office initiating the procurement action or with the COR, the existing DD Form 254 throughout the term of the contract and at least once every two years.

5. Issue a final DD Form 254 to DSS upon completion for the contract with disposition instructions for classified information the contractor possesses pertaining to the Departmental contract.
6. Immediately report to the Security Contact or Servicing Security Office, the contractor's -intent to make public release of classified information, disclosure of classified information, and any occurrence of such activity for which prior written approval of the contracting officer or appropriate visit authorization was not received.

C. The Security Contact/SSO shall perform the following functions:

1. Maintain records of contractor and consultant personnel in any unit subject to the NISP.
2. Provide assistance and guidance to the committee control officer, contracting officer, and COR with respect to industrial security matters.
3. Coordinate the personnel security processing of contractors through the Facility Security Officer of the contractor's employer.
4. Ensure that all contractor and consultant personnel have been briefed on the procedures for handling and safeguarding classified information.
5. Forward a copy of all revised DD Form 254 to the OSY/CED immediately following receipt of revisions from the contracting officer.
6. Verify facility and personnel security clearances of contract personnel through OSY/CED.

Chapter 38. Overseas Security

38.1. Overview

This chapter identifies the overseas physical security policy for the protection of the International Trade Administration (ITA), U.S. & Foreign Commercial Service (US&FCS) employees, facilities, Classified National Security Information (NSI), and sensitive information. This chapter may be amended at any time with the concurrence of Deputy Assistant Secretary (DAS) for the Office of International Operations (OIO), and the Director for Security (Director).

38.2. Primary Responsibilities

A. The OIO Security Team has primary responsibility for interpreting, supplementing, and developing physical security policy, and for oversight of US&FCS office physical security enhancements. The OIO Security Team consists of representatives of OIO and OSY. The team may be contacted through the OIO/DAS at 202-482-6228.

B. US&FCS Bureaus and Offices are responsible for notifying the OIO Security Team when any action is contemplated that will affect US&FCS use of office space.

C. US&FCS Senior Managers, DAS, Regional Directors (RDs), Senior Commercial Officers (SCOs), Principal Commercial Officers (PCOs), and Country Officers are responsible for ensuring that all employees and contractors coming under their authority are aware of and follow the US&FCS security policies and procedures contained in this chapter.

D. SCOs and PCOs are responsible for coordinating security activities within their respective US&FCS Bureaus and Offices with the Bureau of Diplomatic Security (DS) Regional Security Officer (RSO). In addition, SCOs and PCOs are responsible for communicating post-specific security information to the OIO Security Team.

E. All US&FCS employees and contractors are responsible for complying with US&FCS security policies and procedures.

38.3. Policy and Procedures

A. Office Building Security.

1. The OIO Security Team must be notified of any potential action that may affect the use of office space, such as:
   a. US&FCS openings, closings, or relocations
   b. Staff increases or decreases
   c. Other activities necessitating changes in the physical security provisions for office space
2. US&FCS Offices must not sign any lease to acquire additional office space in existing facilities, relocate to new office buildings, construct new offices, or acquire any other type of functional space without the prior written approval of the OIO Security Team.

3. Prior to lease approval, the post must ensure that a site survey is performed by the OIO Security Team or the RSO to determine whether the facility can be brought up to the minimum security standards described in 12 Foreign Affairs Handbook (FAH) 5, Physical Security Handbook and 12 FAH-6, OSPB Security Standards and Policy Handbook. The post must then follow procedures (in coordination with the RSO) as set forth in 12 FAH-5 H-200 for any exception requests. The OIO Security Team designs physical security systems in consultation with the US&FCS Field Office, Regional Office, the RSO, and other appropriate offices in Washington, D.C., both at the Department of Commerce and at the Department of State (DOS).

B. Physical Security Standards. All physical security standards must be met in existing offices, newly acquired offices, and other functional space whether acquired for long-term lease or short-term lease, unless otherwise specified in the DOS standards of 12 FAH 5 and 6. This policy applies to stand-alone facilities, commercial office space, and embassy, consulate, and annex buildings. US&FCS offices must not occupy new facilities until the OIO Security Team grants written approval.

1. The standards in 12 FAH-5 and 12 FAH-6 are modified for US&FCS as follows:
   a. In all situations where 12 FAH-5 calls for a 5-minute forced entry (FE) standard for doors, the 15-minute FE and ballistic resistant standard may be used.
   b. In all situations where 12 FAH-5 calls for a 5-minute FE standard for window grills, the 15-minute FE standard may be used.
   c. In all situations where 12 FAH-5 calls for a 5-minute FE standard for construction, the 15-minute FE standard may be used.
   d. All newly acquired US&FCS office space that includes more than one floor or multiple sections of one floor of a building must be contiguous.
   e. US&FCS must not occupy more than 25 percent of a commercial office building. The percentage refers to the square footage of the space occupied in the building as well as to the ratio of US&FCS staff in the building.
   f. US&FCS safe areas and safe havens must accommodate a minimum of 75 percent of the US&FCS staff and be designed for a minimum of 10 square feet per person.
   g. Alteration, removal, disabling, modification, or movement of US&FCS security systems and components is not authorized without the written concurrence of the RSO and written approval of the OIO Security Team. Security systems and components include, but are not limited to, inspection and screening areas, public access control area, doors and windows, emergency exit doors, locking hardware, alarm systems, closed circuit TV systems, and metal and package screening devices.

C. Exception Requests.

1. Requests for exceptions to physical security standards must be handled in accordance with the policies and procedures outlined in this chapter and 12 FAH-5 H-200. Exception requests must include all of the following information:

a. Identification of the specific standard(s) to be waived.
b. Justification for the exception
c. Statement of the agency's operational requirements
d. Permits
e. Site plan, maps, and photographs
f. Floor plan
g. Description of the building
h. Description of existing security measures
i. Chief of Mission and RSO comments and recommendations

2. The OIO Security Team must evaluate the package for completeness and technical viability. The OIO Security Team evaluation will be forwarded to the Regional Office for comments. It will then be sent to the Director General for approval or disapproval. If approved, the package will be forwarded to DS for a final decision.

D. US&FCS Internal Security Procedures.

1. US&FCS SCOs must ensure that current security procedures are in accordance with OIO, Chief of Mission, and RSO policies and procedures as outlined in the Embassy/Consulate Emergency Action Plan.

2. US&FCS offices are required to hold, at a minimum, semi-annual security drills to practice emergency procedures in the event of a fire, bomb threat, or civil disturbance.

E. Security Assessments at US&FCS Non-collocated Posts.

1. The US&FCS/OIO Security Team will conduct a security assessment at each non-collocated post (where the commercial service is located outside of Embassy/Consulate buildings) at least once every three years (more if a particular post's security situation warrants or if the post moves or some other noteworthy event occurs), subject to availability of funds.

2. The assessment will be arranged in consultation with post.

3. The assessment will consist of a physical inspection of the office space and building and meetings with the SCO, RSO, and Engineering Services Center.

4. After the assessment takes place, the US&FCS/OIO Security Team will generate recommendations for physical security upgrades at post. The US&FCS/OIO Security Team will fund the upgrades, subject to availability of funds.

5. The US&FCS/OIO Security Team will monitor the progress of the post's implementation of the recommendations and facilitate an expeditious completion.

F. Overseas Security Funding. Overseas security budget and funding must be handled in accordance with the policies and procedures outlined in this chapter. US&FCS field offices shall e-mail the OIO Security Team with any requests for security funding.

G. Overseas Residential Security and Local Guard Programs.

1. The DOS administers the Overseas Residential Security and Local Guard Programs through the RSO at post. Refer to 12 FAH-6, which is available through the RSO. US&FCS participation in these programs is in accordance with the policies and procedures contained in this chapter.

2. When residential security standards are not met, the Regional Office must document security needs and request residential security upgrades and/or funding assistance from the RSO. Where security upgrades and/or funding cannot be provided by the RSO, US&FCS offices may request funding assistance from the OIO Security Team. Such requests must be accompanied by an RSO statement that DOS funds are not available.

H. Department of State Residential Security Program Funding Restrictions. DOS funding for the residential security program applies only to U.S. direct-hire employees.

I. Maintenance.

1. Posts must maintain all physical security equipment provided by the OIO Security Team. The SCO must ensure that preventive maintenance is applied to all systems.

2. The RSO must be notified by the SCO when maintenance needs are beyond the capabilities of the US&FCS staff. Arrangements will be made to obtain the assistance of DOS DS assets. In the event that the RSO cannot provide assistance within a reasonable period of time, the SCO may contact the OIO Security Team for assistance.

J. Locks, Keys, and Combination Controls. Locks, keys, and combination controls within US&FCS must be handled in conformance with the policies and procedures outlined in this chapter and 12 Foreign Affairs Manual (FAM). RSO approval is required prior to the installation, modification, or removal of any security locking devices used for the protection of NSI and all entrance and exit doors in any US&FCS facility. For US&FCS Bureaus and Offices that are authorized to store NSI materials, refer to12 FAM 446, Unclassified Office Facility Lock and Leave (L&L) Policy.)

1. **Keys.** Principal and alternate key custodians must be appointed for each US&FCS office.

   a. The key custodian must conduct a quarterly key inventory. The inventory results must be available for the OIO Security Team's inspection.
   b. Accountable keys must be marked "US Govt—Do Not Dupl." Cutting codes or other markings that could aid a locksmith in duplicating keys must be stored in a security container for reference.

2. **Combinations.** The combinations on all security equipment must be changed under the same criteria as those used for combinations on security containers as stipulated in 12 FAM 532, Locks. The Unit Security Officer must maintain a central record of

all combinations within the US&FCS post and ensure that the RSO is provided a copy of the up-to-date central record.

K. Terrorist and Criminal Incident Reporting. The post must report all terrorist and criminal incidents affecting US&FCS employees, contractors, and their dependents (overseas) to the OIO Security Team after appropriate local notification of the RSO. The Duty Officer must always be notified. Requirements for handling NSI must be followed at all times. At overseas posts, a report must be sent, within 24 hours of an incident, to the OIO Security Team by telephone, e-mail, facsimile, cable, or memorandum, and must include all of the following:

1. A summary of the incident
2. Date and local time the incident occurred
3. Location of affected facilities
4. Type of incident
5. Number, identification, and affiliation of personnel affected by the incident
6. Effect of the incident on US&FCS operations
7. Identification of damaged equipment
8. Estimated cost and time to repair or replace the equipment
9. Response of host government forces

38.4. MANDATORY REFERENCES FOR OVERSEAS SECURITY

A. 14 FAM 410, Personal Property Management for Posts Abroad

B. 15 FAM 312, Leasing Policy

C. 12 FAM 300, Physical Security Programs

D. 12 FAM 446, Unclassified Office Facility Lock and Leave (L&L) Policy.

E. 12 FAM 532, Locks

F. 12 FAH-5, Physical Security Handbook

G. 12 FAH-6, OSPB Security Standards and Policy Handbook

38.5. ARMORED VEHICLE PROGRAM

A. Overview. This chapter establishes the policies and procedures for the US&FCS overseas Armored Vehicle Program.

B. Primary Responsibilities. The OIO Security Team has overall responsibility for the US&FCS Armored Vehicle Program. The program is implemented in coordination with DOS' DS and the US&FCS OIO Security Team. The OIO Security Team is responsible for the procurement and shipment of armored vehicles, as well as the cost of applying the armor. The post is responsible for ordinary maintenance of armored vehicles.

C. Policies and Procedures.

1. **Armored Vehicle Procurement and Assignment.**
   a. Armored vehicles must be procured and assigned based on threat and in accordance with 12 FAM 380 Armored Vehicle Program, 12 FAH-6, and the policy and procedures of this chapter.
   b. Armored vehicles will be purchased with OIO Security funds, and the OIO Security Team has the authority to reassign or transfer them between US&FCS posts based on operational and security requirements. Armored vehicles are considered part of the Mission fleet for reporting purposes. US&FCS Bureaus and Offices must obtain RSO and post Emergency Action Committee concurrence prior to requesting the purchase of an armored vehicle.
2. **Armored Vehicle Purchase.**
   a. US&FCS posts must inform the OIO Security Team of their projected armored vehicle requirements during the formulation of the annual budget.
   b. Posts that need to procure an armored vehicle must notify the OIO Security Team and must include the manufacturer, type of vehicle, and any other requests pertaining to the vehicle.
   c. Issues concerning the Armored Vehicle Program shall be directed to the OIO Security Team.
   d. The OIO Security Team will coordinate shipment of the armored vehicle to the overseas post.
3. **Armored Vehicle Usage.**
   a. Armored vehicles at collocated posts (where the commercial service is located within State Department facilities) shall be used for official purposes only. Requests for exceptions to this policy must be submitted to the RSO for approval. For non-collocated posts, the post should seek guidance from the RSO and submit requests to the OIO Security Team for final approval.
   b. Posts must ensure that drivers of armored vehicles are schooled in defensive driving techniques and trained in the unique handling and special characteristics of armored vehicles. Drivers of fully armored vehicles are not permitted to operate that vehicle without supervision until the requisite defensive and related training is received.
4. **Armored Vehicle Protection.** Armored vehicles must not be left unattended when they are outside a U.S.-controlled motor pool unless parked at regularly designated (i.e., overnight) parking area.
5. **Armored Vehicle Maintenance.** The post is responsible for the regular maintenance required on armored vehicles.

6. **Armored Vehicle Disposition.**

   a. US&FCS Bureaus and Offices may dispose of armored vehicles when authorized by the RSO. Armored vehicles must be disposed of in accordance with the policies and procedures outlined in this chapter, 12 FAM 380, and 12 FAH-6. Salvageable radios, usable security alarms, and any other security equipment must be removed before disposal. Where feasible, any polycarbonate window inserts must be removed from armored vehicles prior to disposition.

   b. Any other issues pertaining to armored vehicles not covered in this guidance should be addressed to the OIO Security Team.

D. Mandatory References for Armored Vehicles.

1. 12 FAM 380, Armored Vehicle Program.
2. 12 FAH-6, OSPB Security Standards and Policy Handbook.

Chapter 39. Facility Security Plan Handbook

39.1. BACKGROUND

The National Terrorism Advisory System, or NTAS, replaced the color-coded Homeland Security Advisory System (HSAS). This new system more effectively communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports, other transportation hubs, and the private sector. It recognizes that Americans all share responsibility for the nation's security, and should always be aware of the heightened risk of terrorist attack in the United States and what should be done.

NTAS ALERTS

An individual threat alert is issued for a specific time period and then automatically expires. It may be extended if new information becomes available or the threat evolves. Threat alert types are:

A. **Imminent Threat Alert:** Warns of a credible, specific, and impending terrorist threat against the United States.

B. **Elevated Threat Alert:** Warns of a credible terrorist threat against the United States.

After reviewing the available information, the Secretary of Homeland Security will decide, in coordination with other Federal entities, whether an NTAS Alert should be issued.

NTAS Alerts will only be issued when credible information is available.

These alerts will include a clear statement that there is an **imminent threat** or **elevated threat**. Using available information, the alerts will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses and governments can take to help prevent, mitigate or respond to the threat.

The NTAS Alerts will be based on the nature of the threat: in some cases, alerts will be sent directly to law enforcement or affected areas of the private sector, while in others, alerts will be issued more broadly to the American people through both official and media channels.

NTAS Alerts contain a **sunset provision** indicating a specific date when the alert expires - there will not be a constant NTAS Alert or blanket warning that there is an overarching threat. If threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS Alert. All changes, including the announcement that cancels an NTAS Alert, will be distributed the same way as the original alert.

39.2. PROGRAM OBJECTIVES

DOC senior-level bureau officials and facility managers are required to become familiar with the NTAS Threat Alerts and to develop a Facility Security Plan that will address the NTAS Threat Alerts.

The Department adopted the DHS, ISC Physical Security Criteria for Federal Facilities (Final Draft) dated April 10, 2010 as the *minimum security standards* for all Department-controlled facilities. Department senior-level bureau officials and facility managers are responsible to know their facility security level (FSL), implement the ISC criteria for their facility, and evaluate, identify, and implement additional security measures based on specific mission and critical asset protection requirements.

39.3. AUTHORITY

DOC Facility Security Plan:

- ISC Physical Security Criteria for Federal Facilities (Final Draft) dated April 10, 2010.
- ISC Standard for Facility Security Level Determinations for Federal Facilities dated January 14, 2008.
- NIST Special Publication 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), dated November 2008.
- Presidential Decision Directive 39 (PDD 39), U.S. Policy on Counterterrorism.
- Department of Defense Instruction (DoDI) 2000.16 (DoD Anti-Terrorism Program Standards).

39.4. FACILITY SECURITY PLAN DEVELOPMENT

A. **Overview.** To minimize the risk of any incidents or threats to DOC personnel or facilities and to provide a safe and secure environment that is as responsive as it is practical to mission requirements, appropriate security measures must be developed that correspond to the NTAS Threat Alerts. The development of facility security plan procedures provides the senior-level bureau officials and facility managers with the ability to immediately increase their level of protection (LOP) to a higher LOP to manage the risks associated with the NTAS Threat Alerts. Facility managers must understand what the NTAS Threat Alerts mean at their respective facility. Senior-level officials and facility managers are required to develop security plans and procedures for their facility. These procedures will be incorporated into the facility Occupation Emergency Plan (OEP) and the Continuity of Operations Plan (COOP).

B. Senior-level bureau officials and facility managers have the authority to raise the LOP of their facility to correspond with the NTAS Threat Alerts, local threat conditions or to provide added security measures during periods of potential threat from outside activities or groups. For assistance in applying the ISC LOP to a particular facility, they should contact their DOC Servicing Security Officer (SSO) or the DOC OSY headquarters.

C. Procedures.

1. **Step 1. Determine the ISC Facility Security Level (FSL) for Federal Facilities:** Each DOC facility must be assessed to determine the FSL and LOP based on the ISC Standard. In most cases the, ISC FSL was determined during a previous Anti-Terrorism Risk Assessment. The senior-level bureau official or facility manager should contact the SSO for that information or to discuss the FSL determination for new DOC-owned or GSA leased facilities.
2. **Step 2. Identify Assets to Be Protected:** The senior-level bureau official and facility manager will identify the assets to be protected. Assets are normally assigned to five categories: People, Facilities, Operational Equipment, Information, and Personal Property. Determine whether each asset is critical or non-critical to the organization's mission.
3. **Step 3. Review and Evaluate the ISC Physical Security Criteria for Federal Facilities for Compliance and Effectiveness:** The ISC Physical Security Criteria for Federal Facilities established 62 security criteria in the categories of Site Security Criteria, Structure Security Criteria, Facility Entrance Security Criteria, Interior Security Criteria, Security Systems Criteria, and Security Operations and Administration Criteria to be considered for a facility based on its assessed ISC FSL. The ISC Physical Security Criteria for Federal Facilities establishes the tables to identify the LOP applicable to each facility based on its designated ISC FSL. For example, control of facility parking is recommended as Site Security Criteria for facilities in security level III through V and recommended as "No special measures required" for facilities in security levels I and II.
   a. After determining the facility's ISC FSL and reviewing the LOP, evaluate each security criteria for compliance and implement those security criteria that are necessary for the facility. Senior-level bureau officials and facility managers are encouraged to contact their SSOs to assist in this process.
   b. The ISC security criteria may not adequately provide the appropriate level of protection for all the facility's assets. Senior-level bureau officials and facility managers shall evaluate, identify, and implement additional site-specific security criteria as necessary. These additional security criteria will become part of the facility's site-specific security criteria and facility security plan.
4. **Step 4. Develop a Facility Security Plan:** Senior-level bureau officials and facility managers are required to develop a written facility security plan that specifically addresses the NTAS Threat Alerts. The plan should include at a minimum:
   - Identify security responsibilities

- Identify current and planned security measures
- Define facility-specific security responsibilities
- Contains emergency contacts (such a law enforcement, first responders, security organization, and facility manager)
- Detail response procedures for emergencies
- Outline approved protocols for access by employees, contractors, and visitors
- Established changes in security operations due to NTAS
- Outline the security measure testing schedule performed by the security manager at level IV and V facilities
- Identify security support requirements for the OEP

Note: The level of detail to which the plan is written may vary based on the nature of the facility (e.g. Level I facilities may have abbreviated documents).

At a minimum, this plan should be annotated as "For Official Use Only".

5. **Step 5. Incorporate the Facility Security Plan into the Occupant Emergency Plan:** The facility security plan must be incorporated into the facility OEP and become part of the COOP.
6. **Step 6. Establish an Education and Awareness Training Plan:** Security, emergency management staff, or facility managers, employees, and contractors who have designated responsibilities in the facility security plan must receive training so they fully understand the Facility Security Plan and their individual roles and responsibilities.
7. **Step 7. Provide Continual Review of the Program:** Senior-level bureau officials and facility managers will review and update their facility security plan annually or more often as threat, mission, or operational changes dictate.

Chapter 40. Anti-Terrorism Risk Assessment Program

40.1. PROGRAM OBJECTIVES

A. The Anti-Terrorism (AT) risk management process (an evaluation of impact, threat, and vulnerability) assesses the risk to Department of Commerce (Department) facilities. The Anti-Terrorism Risk Assessments (ATRA) are conducted locally and lay the foundation for senior-level bureau officials and facility managers to make informed decisions and commit scarce resources toward risk minimization.

B. Anti-Terrorism Risk Management Process. The Office of Security (OSY) conducts the ATRA only after completing the Risk Management Process outlined in section 40.3.A. Any plan that does not start with this process shall be too reactive and potentially result in wasted efforts and resources. Determining the AT risk is essential because senior-level bureau officials and facility manages must understand the threat, what assets are most important to protect, and which of those important assets are most vulnerable. Assessing AT risk provides the value of an asset in relation to the AT threats and the vulnerabilities associated with it. This aids senior-level bureau officials and facility managers in balancing threats to vulnerabilities and the degree of risk they are willing to accept by not correcting a vulnerability, or perhaps being unable to correct a vulnerability. For any vulnerability, senior-level bureau officials and facility managers shall manage risk by developing a strategy to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.

C. The purpose of the ATRA Program is to establish an analytical ATRA process to evaluate security standards of new and existing Department- owned and leased facilities. This process will facilitate compliance with the minimum security standards and required actions based on source directives such as the Department of Homeland Security (DHS), Interagency Security Committee (ISC) Physical Security Criteria for Federal Facilities dated April 12, 2010, the ISC Facility Security Level Determinations for Federal Facilities dated January 14, 2008, Department of Commerce Security Manual Policies and Procedures, **Code of Federal Regulations**, and General Services Administration **(GSA) property requirements**.

D. The ATRA Program is designed to protect Department personnel, on-site contractors, visitors, facilities, information, critical infrastructure, and other material resources from terrorist and other criminal acts (e.g., foreign intelligence, workplace violence, riots, and burglary). This is different from the physical security survey, which deals specifically with physical security functions such as protection of classified work areas, weapons, finances, drugs, high-risk equipment, etc.

E. Based on the ATRA Program, senior-level bureau officials, and facility managers will have a detailed list of the current countermeasures in place at their facilities and a full description of the recommended countermeasures to mitigate the vulnerabilities.

F. The ATRA Program provides an overview of the following Department programs:

1. Occupant Emergency Plan (OEP) (See Chapter 7, Occupant Emergency Plans and Procedures).
2. Information Technology (IT) Security Plans (See Department IT Security Policy, CITR-018 IT Security Plans of Action and Milestones).
3. Fire and Safety Equipment (See Chapter 7, Occupant Emergency Plans and Procedures).
4. Foreign National Visitor and Guest Worker Policy (See DAO 207-12, Foreign National Visitor and Guest Access Program).
5. National Security Information (NSI) Accountability and Storage (See Chapter 33, Storage and Destruction Equipment).
6. Communications Security (COMSEC) Equipment Accountability and Storage (See National Security Agency [NSA]/Central Security Service Policy Manual 3-16 dated August 2005).
7. Weapons and Ammunition Accountability and Storage (See Chapter 33, Storage and Destruction Equipment).
8. Security Force Contract Guard Services.

G. The ATRA Program is designed to assess all Department-owned and leased facilities (including new construction, major modernizations, purchases, and new lease acquisitions), Facility Security Level (FSL) I and II within a five-year cycle and all FSL levels III and IV facilities within a three-year cycle.

40.2. AUTHORITY

The Department ATRA Program is guided by:

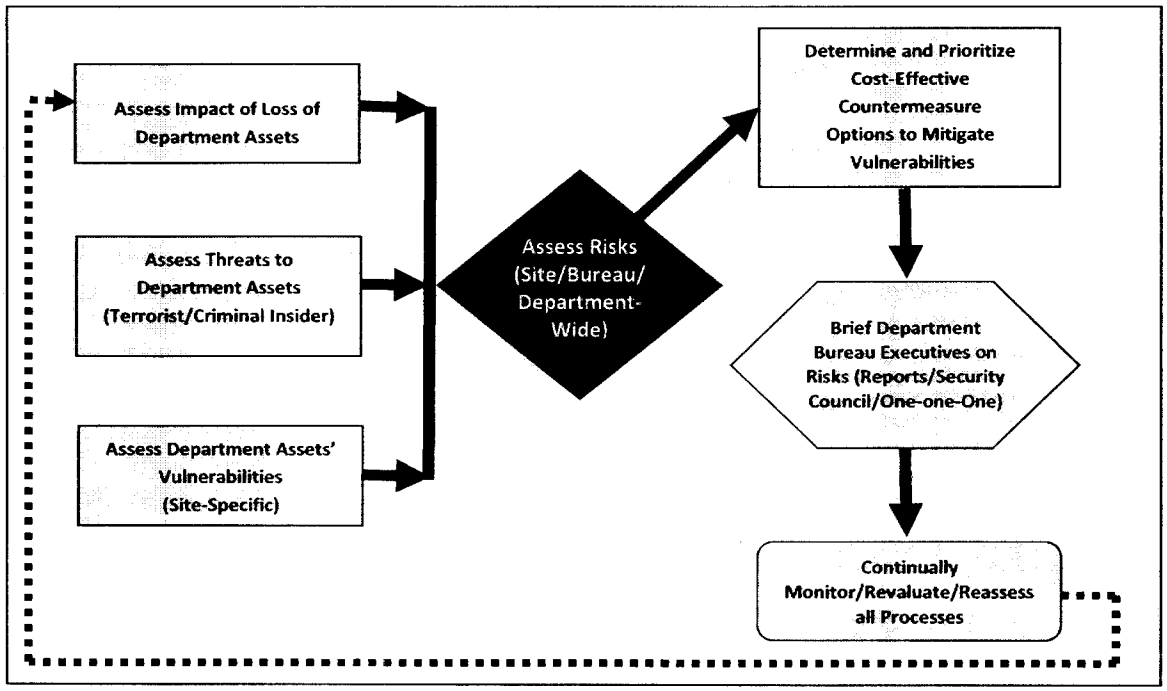
- Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, dated December 2003.
- HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 2004.
- NIST Special Publication 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), dated November 2008
- Presidential Decision Directive 39 (PDD 39), U.S. Policy on Counterterrorism.
- ISC Physical Security Criteria for Federal Facilities dated April 12, 2010.
- ISC Use of Physical Security Performance Measures dated 2009.
- ISC Standard for Facility Security Level Determinations for Federal Facilities dated January 14, 2008.

40.3. METHODOLOGY

A. The ATRAs are based on the Analytical Risk Management (ARM) methodology. The ARM methodology is a systems approach to assessing the impact of, threat to, and vulnerabilities of Department assets listed as people, IT systems, corporate knowledge, equipment, facilities, and information. It is applied against potential undesirable events such as criminal events, terrorist attacks, natural disasters, workplace violence, power failure, hacking and viruses, no off-site storage for backup tapes, no redundancy in network systems, and theft or unintentional loss of information due to natural disaster or terrorist attack. The Servicing Security Office (SSO) assessment collects information and recommends a series of cost-effective countermeasures to protect the Department's assets.

B. The following diagram depicts the ATRA Management Concept. The SSO will assess the risk to a Department facility by examining the following areas: impact on the Department if it suffered operational capability, any potential threat(s), and any site-specific vulnerability. The SSO will provide recommended countermeasures to mitigate the vulnerabilities. Bureau executives will have an opportunity to review the recommendations, select and approve as needed and most important, fund the corrective measure. This process is continually reviewed and updated as needed.

OSY ATRA Management Concept



C. The OSY SSO conducting the ATRA will determine and prioritize the most cost-effective countermeasure options to mitigate the vulnerabilities. Bureau officials and facility managers will be briefed by the SSO on the facility status so they can decide whether they will approve the countermeasure, fund the expense, and complete installation. Recommended countermeasures are continually monitored by the OSY Physical Security Program Manager and SSOs for status updates. A countermeasure recommendation data spreadsheet is maintained on all facilities that receive an ATRA; four months following the initial assessment and periodically thereafter, these countermeasures are reviewed by OSY to update the project status in accordance with the ISC Use of Physical Security Performance Measures criteria for implementing countermeasure recommendations.

D. Once the three or five-year cycle is completed, the assessment cycle repeats based on the predetermined facility schedule for periodic ATRAs.

40.4. MINIMUM SECURITY STANDARDS

The Department adopted the DHS, ISC Physical Security Criteria for Federal Facilities dated April 12, 2010, and the ISC Facility Security Level Determinations for Federal Facilities dated January 14, 2008, as the *minimum security standards* for all Department-controlled facilities. Department senior facility managers are responsible to know their facility security level (FSL), implement the ISC criteria for their facility, and evaluate, identify, and implement additional security measures based on specific mission and critical assets protection requirements.

40.5. SECURITY LEVELS

The ISC FSL establishes three or five security levels as a way to determine the assessment schedule for each Department facility within each five-year cycle. The five ISC FSLs are:

A. ISC FSL I facilities generally have 100 or fewer federal employees and less than 10,000 square feet. Other factors considered are Mission Criticality, Symbolism, Threat to Tenant Agencies, and Intangible Adjustment. FSL I facilities receive an ATRA at least once every five years.

B. ISC FSL II facilities generally have 101 to 250 federal employees and 10,001 to 100,000 square feet. Other factors considered are Mission Criticality, Symbolism, Threat to Tenant Agencies, and Intangible Adjustment. FSL II facilities receive an ATRA at least once every five years.

C. ISC FSL III facilities generally have 251 to 750 federal employees and 100,001 to 250,000 square feet. Other factors considered are Mission Criticality, Symbolism, Threat to Tenant Agencies, and Intangible Adjustment. FSL III facilities receive an ATRA at least once every three years.

D. ISC FSL IV facilities generally have more than 750 federal employees and more than 250,000 square feet. Other factors considered are Mission Criticality, Symbolism, Threat to Tenant Agencies, and Intangible Adjustment. FSL IV facilities receive an ATRA at least once every three years.

E. ISC FSL V facilities. There are no ISC FSL V facilities in the Department's inventory.

F. The Department identifies its Critical Infrastructure facilities as DOC Level 5 facilities because of the criticality and national impact associated with the specific facility's mission. This designation allows OSY to place greater emphasis on the assignment and ranking of overall risk scores for all Departmental facilities. In cases where there is an identified threat or increased risk to Departmental critical infrastructure assets, the designated official, in cooperation with OSY may assign a higher ISC FSL of protection to adequately protect the asset.

G. NOAA vessels (ships) are identified as FSL II facilities; however, NOAA vessels are required to comply with the Department of Homeland Security (DHS) established security measures in accordance with Captain of the Port (COTP) directed U.S. Coast Guard Maritime Security (MARSEC) Levels. Although there is a relationship between the Homeland Security National Terrorism Advisory System (NTAS) and the three Maritime Security Levels, it is important to recognize that the NTAS does not automatically constitute a change of the MARSEC level. The Coast Guard, via the COTP, will evaluate local conditions and when appropriate, directly notify the maritime community of any changes to the MARSEC levels using pre-established methods.

40.6. DEPARTMENT ASSETS AND FACILITIES HOUSED ON US DEPARTMENT OF DEFENSE INSTALLATIONS

Departmental assets and facilities housed on U.S. DOD installations shall comply with security measures in accordance with Combatant Commander directed Anti-Terrorism/Force Protection guidance and Terrorist Force Protection Condition (FPCON) Measures. The FPCON Measures are a Chairman of the Joint Chiefs of Staff-approved program that standardizes the military services' identification of and recommended responses to terrorist threats against U.S. personnel and facilities. This program facilitates inter-service coordination and support for antiterrorism activities and security postures as FPCON.

40.7. DEPARTMENT FACILITIES HOUSED OVERSEAS IN NON-COLLOCATED U.S. DEPARTMENT OF STATE EMBASSIES

Department facilities housed overseas in non-collocated U.S. Department of State Embassies shall comply with the physical security standards outlined by the Overseas Security Policy Board.

40.8. NEW CONSTRUCTION AND PRE-LEASED FACILITIES

Bureau executives and facility managers are strongly advised to consult with their OSY SSOs on security matters relating to Departmental new construction and leased facilities prior to signing formal property agreements. In accordance with the ISC FSL determinations for new leased or owned space, the initial determination will be made as soon as practical after the identification of a space requirement. This determination should be made early enough in the space acquisition process to allow for implementation of required countermeasures (or reconsideration of the

acquisition due to inability to meet minimum physical security requirements). ATRAs of new facilities (including new construction, major modernizations, purchases, and new lease acquisitions) shall be conducted prior to occupancy to ensure the security measures identified in the project planning stage are adequate. For succeeding leases (with no change in tenancy or mission), an ATRA and FSL determination shall be made only if the facility has not already been assessed under the standards specified in the ISC Security Standards for Leased Space. This is to ensure that Department officials receive the appropriate security guidance necessary to accomplish the agreement and avoid unforeseen financial penalties and hardships.

40.9. UNSCHEDULED RISK ASSESSMENTS

ISC FSL I facilities that are collocated in commercial or state facilities through a memorandum of agreement will be given assessment consideration on a case-by-case basis based on the Department having a lease with the lessor.

40.10. REPORTING PROCESS

A. Once the ATRA is completed the SSO will out-brief the facility manager and invited staff officials. The findings and recommendations will be discussed, and a copy of the findings will be provided for their review.

B. The assessment shall be written and forwarded to OSY Anti-terrorism Division (ATD) for review and consultation with the SSO.

C. After the ATRA is complete, OSY ATD will convert the word document to a PDF file and distribute the ATRAs directly to the senior-level bureau officials, their representatives and the SSO. The ATRAs are designated as "For Official Use Only (FOUO)" and are therefore sent via secure file transfer (a software solution that secures and tracks files and messages via encryption). The OSY SSOs, Field Managers, or Field Office Directors will then distribute the assessments to the facility and activity managers.

40.11. DATA ANALYSIS AND FOLLOW-UP

A. OSY requires a written customer consensus/approval on countermeasures (CM) recommendations within 45 days of the ATRAs. The CM status should reflect:

Approved Pending Funding

Approved Funded

Approved in Progress

Completed

None/Not Applicable

Risk Accepted

In accordance with ISC Use of Physical Security Performance Measures, senior-level bureau officials or their representatives have up to 24 months to obtain funding for approved "costly" CM recommendations, and an additional 12 months to purchase,

install, and test the CMs. The ISC process allows 36 months from the date of ATRAs to complete the process.

B. The OSY ATD Physical Security Program Manager will track and continuously compile ATRA data for analysis. The OSY ATD will conduct periodic consultation (at least every 6 months) with bureau executives to discuss program updates and address individual customer concerns.

C. A review of pending countermeasures, approval status, and implementation will assist bureau executives to ensure a safe environment for Department personnel and resources.

SECTION VI. GLOSSARY

Acronyms

AC	Area Command
ADP	Automated Data Processing
ANACI	Access National Agency Check and Inquiries
AOC	Aircraft Operation Center
APO	Army Post Office
ARP	Access Review Panel
ASA	Assistant Secretary for Administration
ATD	Anti-Terrorism Division
ATR	Agency Technical Representative
ATRA	Antiterrorism Risk Assessment
BEA	Bureau of Economic Analysis
BI	Background Investigation
BIS	Bureau of Industry and Security
BMS	Balanced Magnetic Strip
BR	Ballistic Resistant
CAM	Commercial Acquisition Manual
CAR	Commerce Acquisition Regulation
CASU	Cooperative Administrative Support Unit
CBRNE	Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive
CCP	Classified Control Point
CED	Counterespionage Division
CENSUS	Bureau of the Census
CEPD	Continuity and Emergency Preparedness Division
C/FGI-MOD	Confidential Foreign Government Information-Modified Handling Authorized
CFO	Chief Financial Officer
CI	Counterintelligence
CIA	Central Intelligence Agency
CIK	Crypto Ignition Key
CNACI	Childcare National Agency Check with Inquiries
CO	Contracting Officer

COG	Continuity of Government
COM	Chief of Mission
COMSEC	Communications Security
COOP	Continuity of Operations
COP	Continuity of the Presidency
COR	Contracting Officer Representative
CS	Critical Sensitive
CSSD	Client Security Services Division
CSTSA	Cosmic Top Secret Atomal
CT	Counterterrorism
CTS	Cosmic Top Secret
CUI	Controlled Unclassified Information
CUSR	Central U.S. Registry
DAA	Designated Approving Authority
DAO	Departmental Administrative Order
DAS	Deputy Assistant Secretary
DCID	Director of Central Intelligence Directive
DCS	Defense Courier System Service
DHS	Department of Homeland Security
Director	Director for Security
DISCO	Defense Industrial Security Clearance Office
DNI	Director of National Intelligence
DO	Designated Official
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOL	Department of Labor
DOO	Department Organizational Order
DOS	Department of State
DS	Diplomatic Security
DSS	Defense Security Service
DVR	Digital Video Recording
EAC	Emergency Action Committee

EAP	Emergency Action Plan
EAP	Employee Assist Program
EBS	Emergency Broadcast System
EDA	Economic Development Administration
EMSEC	Emanations Security
E.O.	Executive Order
EOC	Emergency Operations Center
EOD	Enter on Duty
EPA	Environmental Protection Agency
e-QIP	Electronic Questionnaires for Investigations Processing
ERT	Emergency Response Team
ESA	Economics and Statistics Administration
ESC	Engineering Services Center
FAA	Federal Aviation Administration
FAH	Foreign Affairs Handbook
FBI	Federal Bureau of Investigation
FCS	Foreign Commercial Service
FEMA	Federal Emergency Management Agency
FGI	Foreign Government Information
FIPC	Federal Investigative Processing Center
FIPS	Federal Information Processing Standard
FIS	Foreign Intelligence Service
FMR	Federal Management Regulation
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPCON	Force Protection Condition
FPO	Fleet Post Office
FPS	Federal Protective Service
FRD	Formerly Restricted Data
FRUS	Foreign Relations of the United States
FSL	Facility Security Level
GAO	Government Accountability Office
GSA	General Services Administration

HAZMAT	Hazardous Material
HCHB	Herbert C. Hoover Building
HR	High Risk
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IACAP	IA Certification and Accreditation Process
IEP	Individual Emergency Plan
IIP	Investigations and Intelligence Programs
IRC	Interagency Referral Center
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
ITA	International Trade Administration
ITSO	Information Technology Security Officer
ITSPP	Information Technology Security Program Policy
JWICS	Joint Worldwide Intelligence Communications System
LBI	Limited Background Investigation
LEO	Law Enforcement Officers
LEPC	Local Emergency Planning Committee
LR	Low Risk
MBI	Minimum Background Investigation
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MR	Moderate Risk
MBDA	Minority Business Development Agency
MSDS	Material Safety Data Sheets
NAC	National Agency Check
NACI	National Agency Check and Inquiries
NACLC	National Agency Check with Law Enforcement and Credit
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NC	NATO Confidential

NCIC	National Crime Information Center
NCS	Non-Critical Sensitive
NDP	National Disclosure Policy
NFPA	National Fire Protection Association
NIACAP	National Information Assurance Certification and Accreditation Process
NICS	National Institute for Chemical Studies
NIMS	National Incident Management System
NIOSH	National Institute of Safety and Health
NIPP	National Infrastructure Protection Plan
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NLETS	National Law Enforcement Telecommunications System
NOAA	National Oceanic and Atmospheric Administration
NOCONTRACT	Not Releasable to Contractors/Consultants
NOFORN	Not Releasable to Foreign Nationals
NR	NATO Restricted
NRP	National Response Plan
NS	NATO Secret
NSA	National Security Agency
NSC	National Security Council
NSI	National Security Information
NSTISSI	National Security Telecommunications and Information System Security Instruction
NTIA	National Telecommunications and Information Administration
NTIS	National Technical Information Services
NU	NATO Unclassified
OCA	Original Classification Authority
OCIO	Office of the Chief Information Officer
OIO	Office of International Operations
OEP	Occupant Emergency Plan
OES	Office of Executive Support
OGC	Office of the General Counsel
OHRM	Office of Human Resources Management
OIG	Office of the Inspector General

OMAO	Office of Marine and Aviation Operations
OMB	Office of Management and Budget
OPF	Official Personnel Folder
OPM	Office of Personnel Management
OPR	Office of Primary Responsibility
OPSEC	Operations Security
ORI	Operational Readiness Inspection
OSHA	Occupational Safety and Health Administration
OS	Office of the Secretary
OSY	Office of Security
PA	Privacy Act
PAD	Public Access Defibrillator
PCO	Principal Commercial Officers
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PIR	Passive Infrared
PMD	Project Management Division
PRI	Periodic Reinvestigation
PUB	Publication
RD	Restricted Data
RFP	Request for Proposal
RFQ	Request for Quotation
ROI	Report of Investigation
RSI	Reimbursable Suitability Investigation
RSO	Regional Security Officer
SAC	Special Agreement Check
SAMD	Strategic and Administrative Management Division
SAO	Senior Agency Official
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCHR	State Criminal History Repository

SCG	Security Classification Guide
SCO	Senior Commercial Officer
SGI	Special Upgrade Investigation
SIP	Shelter-In-Place
SIPRNET	Secret Internet Protocol Network
SS	Special Sensitive
SSAA	System Security Authorization Agreement
SSBI	Single-Scope Background Investigation
SSBI-PR	Single-Scope Background Investigation Periodic Re-Investigation
SSN	Social Security Number
SSO	Servicing Security Officer
SSPCAP	System Security Plan Certification and Accreditation Package
STU	Secure Telephone Units
STE	Secure Telephone Equipment
TA	Threat Analysis or Assessment
TSCM	Technical Surveillance Countermeasures
TS	Top Secret
USC	United States Code
USFA	United States Fire Administration
USFCS	United States and Foreign Commercial Service
USGS	United States Geological Survey
USPTO	United States Patent and Trademark Office
USSAN	United States Security Authority for NATO Affairs
WNINTEL	Warning Notice Intelligence Sources and Methods Involved

Security Terms and Definitions

Access

1. A condition or equipment mode that allows authorized entry into a protected area without alarm by electronically or mechanically deactivating a sensor or sensors.
2. The ability and means to approach, store, or retrieve data, or to communicate with or make use of a resource of an automated data processing system.
3. 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.

Access Control

1. An aspect of security that uses 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 security as a means of controlling movement into or out of secured areas.

Access Control System

An electronic, electro-mechanical, or mechanical system designed to identify and/or admit authorized personnel to the secure area. Identification may be based on any number of factors such as a sequencing of combinations, special keys, badges, fingerprints, signature, voice, and so forth. These systems are for personnel access control only and are not to be used for the protection of stored information or materials.

Accreditation

A formal declaration by a DAA that a system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Adjudication

An examination of a sufficient period of a person's life to make an affirmative determination that the person is suitable for employment or eligible for a security clearance.

Alarm Station

1. A manually activated device installed at a fixed location to transmit a signal such as a concealed holdup button in a bank teller's cage, in response to an alarm condition.
2. A well-marked emergency control unit, installed at a fixed location usually accessible to the public, used to summon help in response to a condition. The control unit contains either a manually activated switch or telephone connected to fire or police headquarters, or a telephone answering service. See also remote station alarm.

Annunciator

1. A device that signals a change of protection zone status in a security system. An annunciator may log alarms or display a continuous status for each alarm sensor in a system. Annunciators include an alarm receiver, alarm monitor, or alarm device.

2. The component of an alarm system that announces a change of status of the system, usually in the form of audible and/or visual signals.

Applicable Associated Markings

Markings, other than those designating a classification level, required to be placed on classified documents. These include the "Derived From" line, downgrading and declassification instructions, special control notices, Special Access Program caveats, and so forth.

Astragal

A member fixed to, or a projection of, an edge of a door or window to cover the joint between the meeting of stiles to prevent access to the lock mechanism.

Automatic Declassification

The declassification of information based upon (1) the occurrence of a specific date or event as determined by the OCA; or (2) the expiration of a maximum time frame for duration of classification established under E.O. 13526.

Balanced Magnetic Contact Switch

A two-part sensor that generates an alarm condition when a change in the magnetic field between the parts is detected. Usually mounted on a door and doorframe to detect opening of the door. A balanced magnetic contact switch provides better protection against a defeat attempt than a standard magnetic contact.

Ballistic Resistance

The capacity of security barriers to defeat a variety of handgun, shotgun, and rifle rounds.

Barbed Wire

Wire, usually of 12 gauge, to which pointed barbs have been added, usually at four-inch/10.16-cm intervals. Barbed wire is often strung along the tops of fences and walls as a deterrent to entry.

Battery Backup

A standby battery that is kept fully charged for use during a primary power failure. The Battery Backup is an essential element of all electrically operated security systems.

Bolt

That part of a lock which, when actuated, is projected (or "thrown") from the lock into a retaining member, such as a strike plate, to prevent a door or window from moving or opening.

Breach

The successful defeat of security controls resulting in a penetration of the system.

Bureau

The operating units of the Department charged with carrying out specified substantive functions (i.e., programs) of the Department (refer to DOO 1-1).

Card Access

A type of access control system that uses a card with a coded area or strip, on or inside the card, to activate a lock or other access control device. To activate the device, the card is inserted into or through a slot where the data in the coded area is read. If the code is accepted, a signal is transmitted to unlock the device or perform some other access control function. See definition of Card Reader for more information on types.

Card Reader

A device that reads the information on a card key. Card readers may obtain data from access cards by reading punched holes, magnetic spots, stripes, or wires, or any of several other methods that use punched, embossed, or embedded information. The reader may be an integral part of the lock, or it can be located in the immediate vicinity. Card readers fall into one of two categories: online or intelligent. Online readers must communicate with a central processor that makes the entry or exit decision and transmits a signal back to the locking device. The intelligent card reader compares the data on the card with preprogrammed parameters, and entry or exit is granted or denied by the card reader itself at the reader location. Intelligent readers are also called stand-alone or offline readers.

Central Alarm or Monitoring and Station

1. An organization or business established for the purpose of monitoring subscribers' alarm systems from a centralized monitoring location rather than at the individual sites.
2. The control point of a monitoring system supervised by security personnel.

Central Station Alarm System

An alarm system that uses a central station as distinguished from a proprietary alarm system where the alarm monitoring is done on site.

Certification

Comprehensive evaluation of the technical and non-technical security features of a system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Change Key

A key that will operate only one lock or a group of keyed alike locks, cylinders, and master key system, as distinguished from a master key.

Classification

The act or process by which information is determined to be classified information (E.O. 13526).

Classification Guidance

Any instruction or source that prescribes the classification of specific information.

Classification Guide

A documentary form of classification guidance issued by an OCA 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.

Classified National Security

Information that has been determined pursuant to E.O. 13526, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Combination

The group of numbers that represent the biting of a key and/or the tumblers of a lock or cylinder.

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.

Compilation

An aggregation of pre-existing unclassified items of information. Compilations of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that qualifies for classification pursuant to E.O. 13526, and is not otherwise revealed by the individual information. Classification by compilation must meet the same standards and criteria as other original classification actions.

Compromise

A probable compromise occurs when (1) classified material is recovered outside of a controlled area, or (2) when the probable controlled area or facility is unattended and not properly secured. In either case, a compromise occurs when the material is accessible to persons who do not possess an appropriate security clearance or a need to know. An actual compromise occurs when, with the conditions identified above, it is determined that the classified information has been released or disclosed to unauthorized person(s) or party(ies) and that damage to national security is deemed likely or determined to have occurred as the result of this unauthorized disclosure. 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.

Confidential Information

Information, the unauthorized disclosure of which could be reasonably expected to cause damage to the national security. The OCA must be able to identify or describe this damage.

Controlled Area

A specifically designated area, such as a room, office, building, or facility where classified information has been authorized for handling, storage, discussion, or processing and supplemental controls have been established that monitor, limit, or control access in accordance with the DAO 207-1, Security Programs.

Controlled Unclassified Information (CUI)

A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 13526, but is (1) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces "Sensitive But Unclassified" (SBU).

Cooperative Administrative Support Unit (CASU)

An organizational unit established within a multi-tenant federal building to manage administrative services for those tenants. The tenant agencies within the building agree to establish the CASU by consolidating the various administrative functions common to most of the tenants.

Damage to 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 (refer to E.O. 13526).

Declassification

The authorized change in the status of information from classified information to unclassified information.

Dedicated Line

1. A power or transmissions line with a single function, such as data transmission or to a single source such as an outlet for a computer.
2. A non-shared telephone line to an individual subscriber from a central station.

Defeat

The successful unauthorized bypassing of an alarm sensor or system so that a protected area can be entered without detection.

Degausser

A device that erases magnetically encoded information from recording tapes, data disks, card keys, recording heads, and other magnetized items.

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 to the source information. Derivative classification includes the classification of information based on classification guidance provided in a Security Classification Guide (SCG). The duplication or reproduction of existing classified information is not derivative classification.

Designated Approving Authority (DAA)

An official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

Deterrent

Any physical or psychological device or method that discourages action. In the physical security arena, locks or window grilles are physical deterrents, and the presence of a guard or surveillance camera are psychological deterrents.

Disable

To temporarily or permanently place a sensor or system out of service.

DOC Persons

Any organization or person, including contractors, guest researchers/scientists, experts, consultants and trainees/students, who have an ongoing official association or that work directly on activities, projects, or programs of the DOC.

Electric Eye

A detector, or detector system, which uses a photoelectric cell to trigger an alarm when the light path between it and its transmitter is interrupted.

Eligibility for Access

A favorable adjudication of an appropriate investigation of the subject's background.

Emergency Exit

A secure door designated for emergency egress during a fire or other life threatening evacuation.

Enter-On-Duty (EOD)
The first day that a new employee or contract employee enters employment or reports to his/her duty station for work.

Event
An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

Facility
A physical structure housing assets necessary to perform a particular function, e.g., a storage facility, a meteorological facility.

Facility Code
A code used in alarm or access control equipment that identifies the customer or location of the equipment.

Fiduciary
An agent or director who stands 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.

Foil
An electrically conductive ribbon used for a sensing circuit.

Forced Entry Resistance
The capacity of security barriers to resist mob attack as outlined in Department of State Certification Standard SD-STD-01.01, Forced Entry and Ballistic Resistance of Structural Systems.

Foreign Contact Reporting
The acquisition, maintenance, and reporting of information concerning instances of official and unofficial contact between Department employees and non-U.S. citizens.

Foreign Government Information
Information provided to the United States 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 (E.O. 13526).

Foreign National
A person born outside the jurisdiction of the United States who is subject to a foreign government and who has not been naturalized under U.S. law.

For Official Use Only
The term used by the DOC to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under E.O. 13526, or its predecessor or successor orders is not to be considered FOUO. FOUO is not classified information.

Fully Armored Vehicles (FAV)

FAVs are treated with ballistic-resistant opaque and transparent armor that afford the occupants protection against high-powered rifle fire.

Grille

A ridged screen or grate mounted over an opening to prevent entry.

Holdup Alarm and System

An alarm that employs a holdup alarm device in which the signal transmission is initiated by the action of the intruder. It is usually a silent alarm to protect the cashier.

Infrared Motion Detector

A passive, low power, area protection device that detects a change in ambient temperature within the coverage pattern caused by the movement of a body. Sensor circuitry generates an alarm when a moving object causes a change in radiated energy levels within the coverage area. These units are more sensitive to objects moving across the beam pattern than to objects moving towards the sensor. Also called passive infrared.

Information

Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of the U.S. Government. See definition for "Control."

Information Assurance (IA)

Information operations (IO) 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 system of policies, procedures, and requirements established under the authority of E.O. 13526, to protect information that if subjected to unauthorized disclosure could reasonably be expected to cause damage to the national security.

Ionization Smoke Sensor

A device able to detect minute smoke particles in the air and provide early warning of a developing fire. These detectors use one or more chambers containing minuscule amounts of radioactive material that ionizes the air in the chamber. Smoke particles entering the chamber are attracted to the ionized air, and the electrical balance between two electrodes is upset, initiating an alarm. Most ionization smoke detectors are fail-safe in that an alarm is initiated if the sensing circuit malfunctions or power fails.

Keeper

The strike plate, mounted in a doorjamb, which receives and retains the bolt of a lock mechanism.

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.

Light Armored Vehicle (LAV)

LAVs are treated with ballistic-resistant opaque and transparent armor materials to afford the occupants protection against handgun fire.

Line Supervision
A method of securing an alarm data line by introducing a continuous impedance or electronic code to the circuit. Breaking or tampering with the line initiates an alarm.

Local Alarm
An alarm that annunciates at the location of a locking device to discourage or announce intrusion attempts. The alarm usually uses a bell, siren, lighting system, or combination of such devices. It usually turns off automatically after a pre-set time, although some require a manual shutoff. A local alarm may also be linked to a central station or other remote location.

Magnetic Contact
A type of sensor that protects a moveable barrier or object such as a door or window. There are two halves which, when separated (by opening the door or window), alters the magnetic field causing the switch to open (or close) the circuit and initiate an alarm.

Microwave
1. Radio waves that have a wavelength less than 30 centimeters and operate at a frequency of 1000 MHz and higher.
2. A type of sensor that uses microwaves to detect motion.
3. A data transmission medium for alarm data.

Mortise Lock
A lock with a threaded cylinder and a bolt operated by a knob or lever designed to be recessed into the edge of a door in a cavity specifically cut out to receive it, which engages a keeper or strike plate set into the door jamb.

Motion Detector
A sensor that detects movement within a protected area by comparing sequential energy transmissions or reflections or ambient energy field levels. Motion detection systems include infrared, microwave, and ultrasonic sensors.

Multiplex Alarm System
An alarm-monitoring system that multiplexes the alarm data reporting. Multiplexing is a communications mode that permits transmission of several signals on a single circuit. Multiplexing is advantageous in large security systems because considerable alarm input information can be transmitted continually without the need for extensive wiring from each sensor to the central station.

National Security
The national defense or foreign relations of the United States (refer to E.O. 13526).

Nuisance Alarm
Activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt.

Open Storage
The storage of sensitive or classified information on shelves or in locked or unlocked non-approved containers or in classified open-storage areas require certification and accreditation when authorized personnel do not occupy the facility.

Operating Unit
Organizational entities charged with carrying out specified substantive functions (i.e.,

programs) of the Department (refer to DOO 1-1).

Original Classification

An initial determination that information requires protection against unauthorized disclosure in the interest of national security (refer to E.O. 13526).

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 (refer to E.O. 13526).

Panic Bar

A quick-release exit bar mounted on a door to permit fast opening in a fire or panic situation. Also called a crash bar.

Photoelectric Alarm

A kind of motion detector that uses a focused beam of light (usually ultraviolet) to detect an intruder. Any interruption in the light path will set off the alarm. The beam is usually aimed so that an intruder would have to break the beam in order to move through the protected area. Sometimes called an electric eye.

Pressure Mat

A thin rubber or vinyl mat that senses intrusions designed for placement under rugs or similar floor coverings. Pressing (stepping) on the mat closes normally open built-in electrical strip switches and initiates an alarm signal. May also be used for non-security applications such as a doorbell actuator.

Redundant

A circuit or system designed to have backup capability in the event of component or equipment failure. Redundant systems have standby components offline and ready for automatic or manual switchover in the event of primary failure.

Remote Station

1. A secondary or auxiliary alarm control located at some distance from the central control station.
2. A digital keypad or card reader that permits local entry and exit.

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.

Re-key

The process of modifying standard key locks or card readers to function with a new key set or facility code.

Rim Cylinder

A cylinder typically used with surface-applied locks and attached with a back plate and machine screws. It has a tailpiece to actuate the lock mechanism.

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. See Security Survey.

Sabotage
The willful destruction or injury of, or defective production of information, material or property of, the government.

Safe
A container, usually equipped with a mounted combination lock, specifically designed for the protection of money, information documents, and other highly negotiable materials or assets.

Secret
The designation applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

Secure Room
A room that offers the same or greater protection than a security container authorized for the storage of classified material through the use of guards, alarms, or locking devices.

Security Contact
An employee within a bureau or operating unit (non-OSY personnel and non-security specialist) whose position's secondary responsibility is to implement and administer the Department's security programs within the operating unit for programs, projects, field sites, facilities, aircraft, or ships.

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 Infraction
A security infraction occurs when classified information is not properly safeguarded in accordance with the DAO 207-1, Security Programs, but does not result in the actual or probable compromise of the material.

Security Manager
A database that enables the Office of Security to effectively manage the Department's personnel pre-appointments, suitability, security clearances, reinvestigations, classified information, and foreign national visitor vetting and approval process.

Security Specialist
As defined by OPM Standards, a person whose primary duties include analytical, planning, advisory, operational, or evaluative work that has, as its principal purpose, the development and implementation of policies, procedures, standards, training, and methods for identifying and protecting information, personnel, property, facilities, operations, or material from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss. A security specialist at times is called upon to provide specialized program guidance or support or to perform compliance reviews.

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, threat, and vulnerability. 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, e.g., locks, security containers, guards, access controls, alarms.

Security Vault

An area approved by the agency head, which is designed and constructed of masonry units or steel-lined construction to provide protection against forced entry.

Security Violation

A security violation occurs when, in the judgment of the investigating official, failure to safeguard classified information could result in the actual or probable compromise of the material.

Senior Agency Official

The official designated by the agency head under E.O. 13526 – Classified National Security Information, and administers the agency's program under which information is classified, safeguarded, and declassified..

Sensitive But Unclassified (SBU)

See "Controlled Unclassified Information (CUI)."

Sensitive Compartmented Information (SCI)

Collaterally classified information involving intelligence sources, methods, and analytical processes. Requires limited access and strict control of its dissemination. SCI is also known as "Codeword" information.

Sensitive Compartmented Information Facility (SCIF)

An accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed.

Servicing Security Officer

A senior security specialist of the Office of Security stationed at either a bureau or operating unit facility and responsible for providing guidance and oversight to operating unit senior managers, program officials, and security contacts on Departmental security programs; also provides security administration services within their jurisdiction.

Shackle

The hinged or sliding part of a padlock that does the fastening.

Slide Bolt

A simple lock operated by hand without using a key, a turn-piece, or other actuating mechanism. Slide bolts normally can be operated only from the side of the door on which they are mounted.

Status

The condition of an alarm zone, sensor, or system at a given time.

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 that 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. Suitability also refers to statutory or regulatory bars that 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, CCTV, or other monitoring methods.

Technical Surveillance Countermeasures (TSCM)
Employment of services, equipment, and techniques designed to locate, identify, and neutralize the effectiveness of technical surveillance activities.

Top Guard
Anti-personnel device, usually of barbed or concertina wire, installed at the tops of fences and along roof edges.

Top Secret (TS)
The designation applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security.

Ultrasonic
Sound waves having a frequency above that of audible sound (approximately 20,000 Hz). Ultrasonic sound is used in ultrasonic detection systems.

Unauthorized Disclosure
A communication or physical transfer of classified information to an unauthorized recipient (refer to E.O. 13526).

Underwriters' Laboratories, Inc. (UL)
A nonprofit, national testing laboratory that tests and certifies various categories of equipment and electrical devices for safety and reliability.

Vibration Detection
An alarm system that employs one or more contact microphones and vibration sensors that are fastened to the surfaces of the area or object being protected to detect excessive levels of vibration.