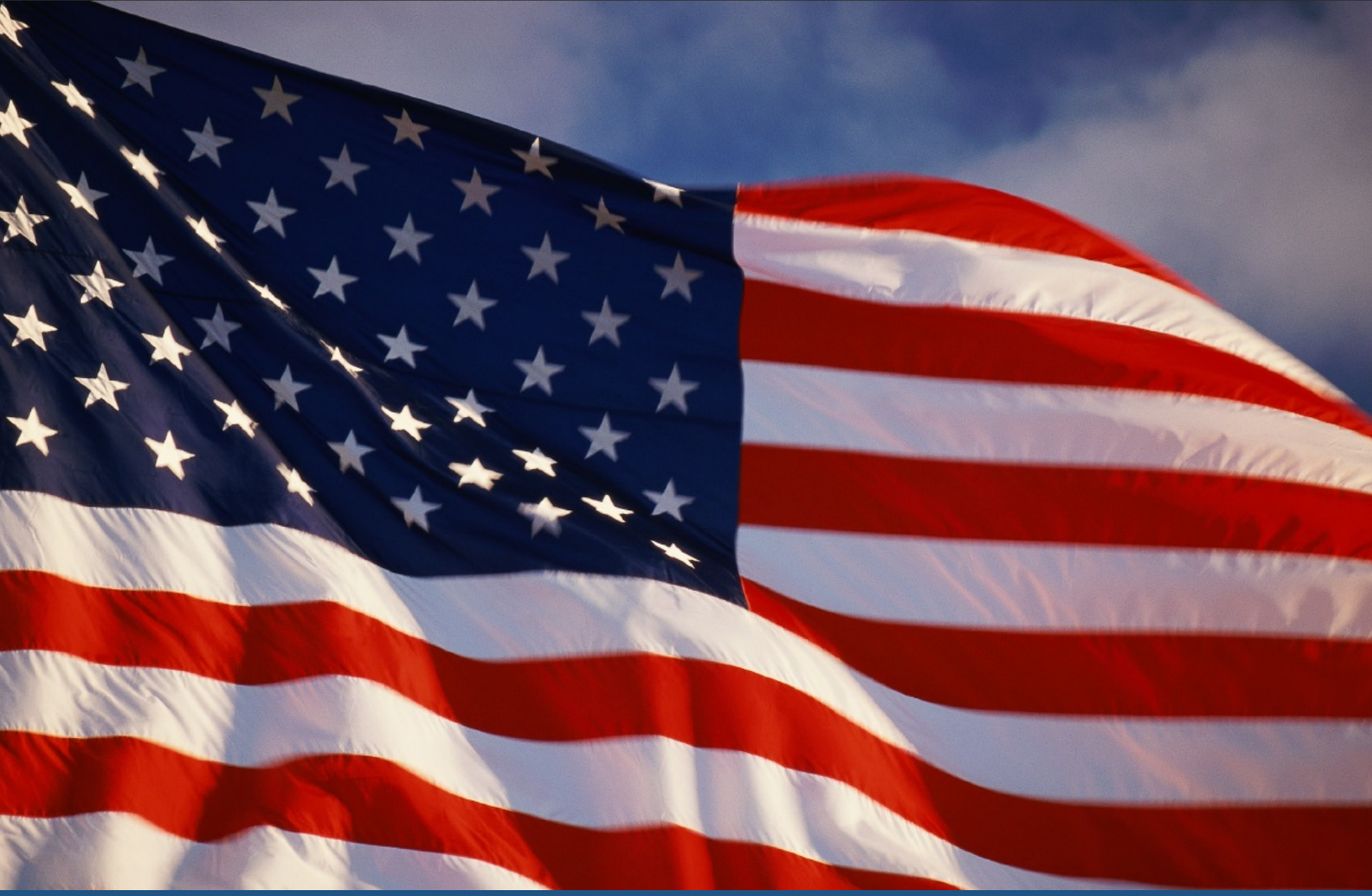

Information Security Handbook

Office of Professional Responsibility
HB 1400-04A

July 2016

U.S. Customs and Border Protection

Foreword

The mission of the U.S. Customs and Border Protection (CBP) is to prevent terrorists and terrorist weapons from entering the United States and to facilitate the flow of legitimate trade and travel across our borders. CBP uses various types of restricted information to accomplish this mission, including classified national security information and sensitive but unclassified information. Protection of such information is of paramount importance; its disclosure to unauthorized individuals, whether deliberate or inadvertent, could result in varying degrees of damage to essential government programs and operations, persons both inside and outside of CBP, and the national security.

The CBP Information Security Handbook establishes CBP policy and guidance on the safeguarding and handling of classified national security information and sensitive but unclassified information throughout CBP. The policies and procedures identified herein are issued in compliance with federal law, executive order, and Department of Homeland Security (DHS) mandate concerning the protection of classified and sensitive information.

This handbook is intended for use by all CBP employees, contractors, and detailees. Its purpose is to guide CBP personnel in properly identifying, handling, and protecting classified and sensitive information that has been entrusted to them in the performance of their official duties and responsibilities.

Security of our critical information is the daily responsibility of all CBP personnel. The integrity of the CBP mission and the capacity to meet the organization's goals is dependent upon our constant vigilance and our ability to safeguard classified and sensitive information from compromise and misuse at the hands of our adversaries. As Component Chief Security Officer for CBP, I fully support the Office of Professional Responsibility in its program oversight activities of CBP's Information Security Program.

For questions or additional information, please contact the Office of Professional Responsibility, Security Management Division, Information Security Branch at CBP.Security@dhs.gov.

Matthew Klein
Assistant Commissioner, Office of Professional Responsibility
Component Chief Security Officer
U.S. Customs and Border Protection

Revision History

Periodic updates to this handbook will be published as necessary to comply with new or revised information security and classification management policies and procedures, including applicable executive orders, regulations, and agency guidance. All revisions will be identified and described in the table below.

Version	Release Date	Description of Change(s)
1.0	September 2015	Initial release.
1.1	July 2016	▪ Replaced all references to "Office of Internal Affairs" and "IA" with "Office of Professional Responsibility" and "OPR," respectively. ▪ Moved general information regarding storage of Sensitive Compartmented Information from section 6.5 to introductory section of Chapter 6. ▪ Incorporated changes to CBP policy requiring program offices that handle and store classified information to: - Conduct annual security container inventories by September 30 of every year (*updated section 5.4, added section 6.11, and revised appendices C and D*); and - Conduct an inventory and turnover process on security containers following the departure of senior CBP officials who had access to such containers (*added section 6.12 and Appendix E., Security Container Turnover Procedures*). ▪ Updated section 6.1.1 and 6.2 to comply with current Federal specifications for new purchases of combination locks and modified section 6.2 to clarify requirements for the storage of Top Secret information and include definition of Security-in-Depth. ▪ Revised policy on the use of DHS Form 11000-10 (Report of Security Incident) (*updated section 8.1 to include that the form is used for reporting security violations and infractions and modified section 8.3.3 to remove that the form is used to provide written statements*). ▪ Applied minor revisions to Appendix A., Classified Meeting Procedures Checklist. ▪ Revised Appendix D., Responsibilities of the Classified Document Custodian, to clarify requirements for maintaining receipts of classified material.

Table of Contents

1. Introduction

1.1. Purpose

This handbook implements Executive Order (E.O.) 13526, *Classified National Security Information*, and Department of Homeland Security (DHS) Instruction 121-01-011, *Administrative Security Program*. It establishes safeguarding, classifying, declassifying, and downgrading requirements for official information requiring protection in the interest of national security and defines procedures for the identification, handling, and protection of unclassified information that is sensitive in nature. The provisions of this handbook set forth the minimum security standards and safeguards to ensure the protection of classified and sensitive but unclassified information within the U.S. Customs and Border Protection (CBP).

1.2. Scope

This handbook is applicable to all persons who are permanently or temporarily employed by, assigned to, or detailed to CBP.

1.3. Authorities

- Public Law 80-235, *National Security Act of 1947*, as amended.
- Public Law 83-703, *Atomic Energy Act of 1954*, as amended.
- Public Law 96-456, *Classified Information Procedures Act*, October 1980.
- Public Law 107-71, *Aviation and Transportation Security Act*, November 2001.
- Public Law 107-295, *Maritime Transportation Security Act of 2002*, as amended.
- Public Law 107-296, *Homeland Security Act of 2002*.
- Title 49 U.S.C. § 114(r), *Nondisclosure of Security Activities.*
- E.O. 12829, *National Industrial Security Program*, January 6, 1993, as amended.
- E.O. 12968, *Access to Classified Information*, August 2, 1995, as amended.
- E.O. 13526, *Classified National Security Information*, December 29, 2009.
- E.O. 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, August 18, 2010.
- Title 6 C.F.R. § 7, *Classified National Security Information*, January 27, 2003, as amended.
- Title 32 C.F.R. § 2001, *Classified National Security Information; Final Rule*.
- Title 32 C.F.R. § 2004, *National Industrial Security Program Directive No. 1*.
- Title 49 C.F.R. § 1520, *Protection of Sensitive Security Information*.

- DHS Instruction 121-01-011, *The Department of Homeland Security Administrative Security Program*, April 2011.
- DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*.
- DHS Management Directive 11056.1, *Sensitive Security Information (SSI)*.
- DHS Delegation No. 8100.5, *Delegation of Original Classification Authority*.
- CBP Directive No. 2130-016, *Roles and Responsibilities for Internal Affairs Activities and Functions.*
- TSA Management Directive 2810.1, *SSI Policies & Procedures Handbook*.
- DOD Manual 5220.22-M, *National Industrial Security Program Operating Manual*, February 2006.

1.4. Responsibilities

1.4.1. Commissioner, U.S. Customs and Border Protection

The Commissioner, CBP, collaborates with the DHS Chief Security Officer in recruiting and selecting the Component Chief Security Officer (CCSO) for CBP.

1.4.2. Assistant Commissioner, Office of Professional Responsibility

The Assistant Commissioner, Office of Professional Responsibility (OPR), as the designated CCSO, serves as the principal advisor to the Commissioner regarding CBP's Information Security Program and ensures sufficient resources are in place to implement and manage the Information Security Program and the requirements of this handbook. The Assistant Commissioner, OPR, also tasks the Director, OPR Security Management Division (SMD), with the responsibility to implement and manage the CBP Information Security Program.

1.4.3. Assistant Commissioners and the Chief, U.S. Border Patrol

Assistant Commissioners and the Chief, U.S. Border Patrol (or other officials as designated), are responsible for appointing, in writing, a primary and alternate Designated Security Officer (DSO) for each sector, field office, air and marine location, and program office (e.g., Office of Human Resources Management, Office of Administration, Office of International Affairs, Office of International Trade) that handles classified and sensitive but unclassified information, as well as a primary and alternate Classified Document Custodian (CDC) for locations where classified information is stored and processed.

1.4.4. Office of Professional Responsibility, Security Management Division

OPR/SMD oversees and administers CBP's classification management and sensitive but unclassified information management programs and the Security Education, Training, and Awareness program. OPR/SMD also issues any necessary procedures required for the effective implementation of this handbook.

1.4.5. Office of Professional Responsibility, Personnel Security Division

The OPR Personnel Security Division (PSD) develops policies and procedures to guide the implementation and administration of the Personnel Security and Suitability program for CBP. OPR/PSD also renders employment suitability determinations and grants security clearances for access to classified national security information, as defined in the CBP Personnel Security Handbook, HB 1400-07A.

1.4.6. Office of Intelligence

The Office of Intelligence is responsible for managing CBP's Sensitive Compartmented Information (SCI) program and granting SCI access to CBP personnel.

1.4.7. Office of Information and Technology

The Office of Information and Technology is responsible for managing CBP's Communications Security (COMSEC) program, accrediting classified information systems, providing information technology security training, and managing CBP systems access requirements, as defined in the CBP Information Systems Security Policies and Procedures Handbook, HB 1400-05D.

1.4.8. Supervisors and Managers

Supervisors and managers must ensure that they and those they supervise are aware of the applicable provisions of this handbook and promote and ensure compliance by staff members. Supervisors and managers must ensure security training is provided upon initial assignment of an employee, detailee, or contractor and is reinforced periodically thereafter through routine office interaction, email reminders, staff meetings, and other office gatherings.

1.4.9. Designated Security Officers

DSOs must ensure that the procedures set forth in this handbook are followed within their respective area of responsibility. DSOs are responsible for providing assistance and support to regional CBP personnel and serve as liaisons to OPR/SMD for applicable matters relating to the implementation of and compliance with the provisions of this handbook.

1.4.10. Classified Document Custodians

CDCs are responsible for security containers within their respective office space, including combinations, document control, and container forms. CDCs must ensure that the movement of classified information outside of their office can be traced, dissemination is limited, prompt retrieval of information can be obtained, the loss of information can be detected, and excessive holding and reproduction of information is limited.

1.4.11. CBP Personnel

All CBP personnel, including employees, detailees, contractors, consultants, and others to whom access is granted, are responsible for protecting classified and sensitive but unclassified information from unauthorized disclosure. All personnel must be aware of and comply with the applicable provisions of this handbook and must report to the

appropriate officials any incidents or violations that affect the safeguarding of classified and sensitive but unclassified information. Personnel must also ensure that their access to and sharing of classified and sensitive but unclassified information is in conjunction with the appropriate level of security clearance, an established need to know, and applicable laws, Federal regulations, and agency policies and procedures.

1.5. Supersession

This handbook supersedes the following:

- CBP Handbook 1400-02B, *CBP Security Policy and Procedures Handbook, Information Security: Safeguarding Classified and Sensitive But Unclassified Information* (Volume 4).

1.6. Contact Information

Questions or comments regarding this handbook may be addressed to OPR/SMD at CBP.Security@dhs.gov.

2. Classification Management

The integrity of CBP's classification management system is dependent upon the knowledge and judgment of CBP personnel who access, disseminate, store, and handle classified national security information. CBP officials involved in the classification process must comply with the standards cited in this handbook to ensure the integrity of the classification management system is maintained.

The Office of Professional Responsibility (OPR), Security Management Division (SMD) has program oversight of CBP's classification management policies, processes, and procedures, as set forth in this handbook. OPR/SMD works closely with the Office of Intelligence (OI), which holds responsibility for the protection of Sensitive Compartmented Information in CBP.

2.1. Original Classification Authority

An original classification authority (OCA) is an official who is authorized, in writing, by the President, by an agency head, or by other officials delegated by the President, to make an initial determination to classify information for national security purposes.

The Secretary of Homeland Security has been delegated by the President as an OCA with the authority to classify eligible information up to and including the Top Secret level. The Secretary can further delegate Top Secret original classification authority to additional DHS officials, pursuant to E.O. 13526. These delegations are identified in DHS Delegation No. 8100.5, *Delegation of Original Classification Authority*.

2.2. CBP OCA Positions

Within CBP, two positions have been delegated original classification authority at the Top Secret level: the Commissioner and the Assistant Commissioner, OI. CBP officials who have been delegated original classification authority cannot further delegate this authority; however, if an individual is exercising the authority of a designated position in an acting or interim capacity, that individual has the authority to classify eligible information.

OCAs at a specified clearance level are also authorized to classify information at lower levels.

The Commissioner may request additional OCA delegations when an operational need exists. Requests for OCA delegations are submitted to the DHS Office of the Chief Security Officer (OCSO), through the Assistant Commissioner, OPR, using DHS Form 11041-1 (Request for Delegation of Original Classification Authority). OCA delegation requests are based on justification of a demonstrated and continuing need for such authority.

CBP officials serving in OCA-delegated positions:

(a) Receive training on OCA responsibilities, methods, and procedures within 60 days of occupying a delegated position and at least once each calendar year thereafter. This specialized training covers proper classification and declassification with an emphasis on the avoidance of over-classification. OPR/SMD is responsible for providing the training. OCAs must sign an acknowledgement that they have received and understand the training prior to taking any original classification action. OCAs who do not receive the mandatory refresher training at least once within a

calendar year will have their original classification authority suspended until completion of such training, unless a temporary waiver has been approved in writing by the Secretary or the DHS Chief Security Officer. Such waivers may not exceed 60 days from the date of issuance.

(b) Communicate original classification decisions through the publication of a security classification guide. When a decision cannot immediately be incorporated into a security classification guide, the decision must be indicated directly on the document as cited in section 3.2 of this handbook. Such decisions must be incorporated into a security classification guide within one year.

(c) Are encouraged to consult with OPR/SMD for assistance when classifying information.

2.3. Original Classification Process

Original classification is the initial determination that information requires protection against unauthorized disclosure in the interest of national security. Information is originally classified under the terms of E.O. 13526 if all of the following conditions are met:

(a) The information is owned by, produced by or for, or under the control of the U.S. Government (Note: For purposes of this handbook, "control" means the authority of CBP to regulate access to the information.);

(b) The information falls within one or more of the categories of information listed in section 2.5 of this handbook and as defined in E.O. 13526;

(c) The OCA determines and can justify that the unauthorized disclosure of the information could reasonably be expected to cause damage to national security, and the OCA is able to identify or describe the damage; and

(d) The OCA classifies the information by determining the appropriate classification level, as defined in section 2.4 of this handbook, and the appropriate duration of classification, as defined in section 2.6 of this handbook.

If there is significant doubt about the need to classify information or at which level, it is not classified, or it is classified at a lower level.

2.4. Classification Levels

National security information that requires protection against unauthorized disclosure is classified by an OCA at one of the following three levels:

(a) Top Secret is 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.

(b) Secret is 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.

(c) Confidential is 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.

2.5. Classification Categories

Information considered for classification must fall into one or more of the categories listed below. The indicator preceding each category is the category identifier defined in E.O. 13526, Section 1.4.

(a) Military plans, weapons systems, or operations;

(b) Foreign government information;

(c) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(d) Foreign relations or foreign activities of the United States, including confidential sources;

(e) Scientific, technological, or economic matters relating to 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; or

(h) The development, production, or use of weapons of mass destruction.

2.6. Duration of Classification

At the time of original classification, the OCA assigns a date or event at which time the information will be downgraded and/or declassified. Upon reaching the date or event, the information is automatically declassified except for information that would clearly and demonstrably be expected to reveal the identity of a confidential human source or key design concepts of a weapon of mass destruction. At the time of classification, the OCA attempts to:

(a) Determine a specific date or event within 10 years of the date of origination, upon which the information can be automatically declassified.

If that is not possible, the OCA attempts to:

(b) Assign a date 10 years from the date of origination at which time the information can be automatically declassified. Should the sensitivity of the information warrant classification beyond a 10-year period, the OCA assigns a date no longer than 25 years from the date of origination at which time the information will be automatically declassified, unless it is reclassified.

No information remains classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders (e.g., information marked as "Originating Agency's Determination Required") or classified information that contains incomplete declassification instructions or lacks declassification instructions is declassified in accordance with section 2.18 of this handbook.

Except for information that clearly and demonstrably reveals a confidential human source or reveals key design concepts of a weapon of mass destruction, which may be classified for up to 75 years, an OCA cannot classify information beyond 25 years unless such information has been specifically approved for exemption from declassification, pursuant to E.O. 13526.

2.7. Communicating Original Classification Decisions

Classification decisions made by an OCA must be communicated through a security classification guide. When a decision cannot immediately be incorporated into a security classification guide, the decision is indicated directly on the document. These decisions must be incorporated into a security classification guide within one year.

2.8. Security Classification Guides

A classification guide is a documentary form of classification decisions issued by an OCA. The guide identifies the elements of information regarding a specific subject that are classified and establishes the level and duration of classification for each element.

CBP offices and/or programs that develop originally classified information must coordinate the development of security classification guides with OPR/SMD and OI. Classification guides must be approved and signed by an OCA and must adhere to the standard DHS format. OPR/SMD will submit final copies of CBP classification guides to the DHS OCSO Administrative Security Division (ASD). For additional guidance on preparing security classification guides, see DHS's *A Guide for Writing a DHS Security Classification Guide*, which covers this topic in detail.

Individuals using classification guides to classify documents do not need to have original classification authority. Appropriately trained and certified CBP personnel who generate information that requires classification based on a classification guide may "classify" the information by citing the applicable authority listed in the guide and applying the classification level specified in the guide. This action is considered derivative classification from a classification guide.

2.9. Classification Prohibitions

Under no circumstances may information be classified, continue to be maintained as classified, or fail to be declassified in order to:

(a) Conceal violations of law, inefficiency, or administrative error;

(b) Prevent embarrassment to a person, organization, or agency;

(c) Restrain competition; or

(d) Prevent or delay the release of information that does not require protection in the interest of national security.

2.10. Classification by Compilation

Compilation of items of information that are individually unclassified may be classified under the following circumstances:

(a) The compilation reveals an additional association or relationship that meets the standards and criteria for classification under E.O. 13526.

(b) The additional association or relationship is not otherwise evident or revealed in the individual items of information.

(c) The information is classified by an OCA.

In these instances, the additional association or relationship is what is considered for classification, not the individual items of unclassified information. Careful consideration must be taken when determining the need for classification by compilation. When the determination is made that classification by compilation is necessary, the OCA must provide explicit instructions as to which elements of the compilation, when combined, require classification and the additional association or relationship that warrants the classification.

OPR/SMD and OI will provide assistance in determining whether information should be classified by compilation.

2.11. Dissemination Controls

OCAs may further associate one or more of the following dissemination controls with their classification decisions:

(a) NOFORN (Not Releasable to Foreign Nationals)

Classified information is not shared with non-U.S. entities unless permitted by the originator. In cases where the OCA has determined that there are no possible circumstances or situations in which the information may be shared with a foreign government, the information must be designated NOFORN to preclude sharing requests. OCAs must carefully consider the consequences of applying the NOFORN designation to information.

(b) ORCON (Originator Controlled)

The application of the ORCON designation requires that further dissemination beyond the headquarters and specified sub-elements of the recipient organization be coordinated with the originating office. For any information that is designated ORCON, the OCA tracks all dissemination of the information. OCAs must carefully consider the consequences of applying the ORCON designation to information.

(c) REL (Releasable to)

The application of REL, followed by the applicable Controlled Access Program Coordination Office (CAPCO)-approved trigraph or tetragraph, indicates that information has been approved to be releasable to the countries or organizations listed. Where applicable, the designation of REL must be done in coordination with the appropriate Foreign Disclosure Office through OPR/SMD.

(d) RELIDO (Release Determined by Foreign Disclosure Official)

The application of the RELIDO marking indicates that the OCA has approved the information to be releasable to foreign countries or organizations at the discretion of an authorized foreign disclosure official.

(e) PROPIN (Caution – Proprietary Information Involved)

The PROPIN marking is used to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value. This marking may be used on government proprietary information only when the information can provide a contractor an unfair advantage, such as U.S. government budget or financial information. Information marked PROPIN is not disseminated to contractors regardless of their status without the explicit authorization of the provider of the information.

2.12. Tentative Classification

If an individual develops information believed to require classification, the individual must safeguard and mark the information in the manner prescribed for its intended classification level. Additionally, the notation "TENTATIVELY CLASSIFIED PENDING AN ORIGINAL CLASSIFICATION DECISION" must be marked prominently and conspicuously on the bottom of each page.

A request for a classification decision must be submitted to the appropriate CBP OCA by a means approved for the intended level of classification, as described in section 7.1 of this handbook. The OCA must notify the sender of a classification determination within 30 days of receiving the request. OPR/SMD will provide guidance as needed to determine the appropriate OCA with subject matter interest.

2.13. Reclassifying Previously Declassified Information

Information may not be reclassified after it has been declassified and released to the public under proper authority unless:

(a) The Secretary approves the reclassification, in writing, based on a document-by-document review and determination that the reclassification is required to prevent significant and demonstrable damage to national security.

(b) The released information may be reasonably recovered and brought back under DHS control without bringing undue attention to it.

(c) The reclassification action is reported within 30 days to the Assistant to the President for National Security Affairs and the Director, Information Security Oversight Office (ISOO).

(d) The Archivist is notified and reclassification is approved by the Director, ISOO, if the information is in the physical custody of the National Archives and Records Administration (NARA) and has been available for public use.

(e) The recipients or holders of the reclassified information who have current security clearances are appropriately briefed about their continuing legal obligations and responsibilities to protect this information from unauthorized disclosure. The recipients or holders who do not have security clearances are, to the extent practicable, appropriately briefed about the reclassification of the information to which they have had access, reminded of their obligation not to disclose the information, and requested to sign an acknowledgement of this briefing.

2.14. Records of Original Classification Actions

Personnel performing original classification actions must maintain a record of each action taken. For originally classified information, the record must include the total number of documents originally classified, by classification level and by declassification date.

Records of original classification actions are counted by document, not by page, and each document must be reported by its overall classification level. For example, a newly created originally classified document consisting of multiple pages and containing both Secret and Confidential information is counted and reported as one originally classified document at the Secret level.

Reports must be submitted annually to OPR/SMD. OPR/SMD will submit one component report to DHS OCSO as part of the annual reporting requirements defined in E.O. 13526 and DHS Instruction 121-01-011.

2.15. Classification Challenges

Authorized holders of classified information who, in good faith, believe a classification status is improper, are encouraged and expected to challenge the classification status. Classification challenges are presented to the classifier of the information. When necessary, assistance and/or anonymity in processing a classification challenge can be obtained by processing the challenge through OPR/SMD. In accordance with E.O. 13526, individuals submitting a classification challenge are not subject to retribution of any kind for bringing such actions.

The OCA receiving the challenge must provide a written response with a classification/declassification decision to the challenger within 60 days of receipt. The individual submitting the challenge has a right to appeal the decision to the Interagency Security Classification Appeals Panel (ISCAP). OPR/SMD will assist with appeals as needed.

Challenged information remains classified and must be protected at its highest level of classification until a final classification determination is made by an appropriate OCA.

2.15.1. Informal Classification Challenges

Classification challenges do not prohibit an authorized holder from informally questioning the classification of information through direct and informal contact with the classifier. When appropriate or when uncertainties exist over the classification status, holders of classified information are encouraged to make direct contact with the classifier to obtain clarification. When a change in classification results from an informal challenge, the challenger must ensure that the official from whom the change was received is authorized to make such a change, and a record of the change, to include the official's name, position, agency, and date must be maintained with a file copy of the document. The OCA making the decision is responsible for notifying holders of the change in classification.

2.15.2. Formal Classification Challenges

Formal challenges to classification must be presented in writing to an OCA having jurisdiction over the challenged information. Every effort should be made to keep the

written correspondence unclassified. However, if the challenge includes classified information, it must be marked and safeguarded accordingly. The written correspondence must sufficiently describe the information being challenged and must consist of only questions as to why the information is classified and why it is classified at a particular level.

2.16. Raising the Classification Level

Classified information may be raised to a higher level of classification only by officials who have been delegated the appropriate level of original classification authority and have cognizance over the information. Action may be taken to raise the level of classification only if holders of the information can be notified of the change so that the information is uniformly protected at the higher level. The OCA making the decision is responsible for notifying holders of the change in classification.

2.17. Derivative Classification

Derivative classification is the process of 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 also includes the classification of information based on guidance provided in a security classification guide.

Restricted Data/Formerly Restricted Data (RD/FRD) derivative classification requires completion of the Department of Energy-approved Restricted Data Derivative Classifier course. This course is offered by the DHS OCSO/ASD Training Branch. For more information on RD/FRD, refer to DHS Instruction 121-01-011, Chapter 6 (Restricted Data and Formerly Restricted Data).

2.17.1. Derivative Classification Authority

Derivative classification authority is tied to an individual or position that has an official need to derivatively classify information. Before being authorized to derivatively classify information, the individual must be identified, trained, and certified based on established DHS standards.

(a) Identification

Supervisors and managers must identify those individuals or positions over which they have cognizance who have a need to derivatively classify information and submit the names of those individuals in writing to OPR/SMD to coordinate training. All individuals with access to classified systems (e.g., Homeland Secure Data Network (HSDN) and/or Joint Worldwide Intelligence Communications System (JWICS) accounts) must be identified as derivative classifiers.

(b) Training

CBP employees who are identified as derivative classifiers must receive initial and refresher training on proper derivative classification, to include the avoidance of over-classification. Derivative classifiers are required to receive refresher training at least once every two years and to report all such training to OPR/SMD upon completion in order to retain their derivative classification authority.

(c) Certification

Prior to certification as a derivative classification authority, individuals must demonstrate that they are aware of proper derivative classification procedures and markings through the completion of training approved by DHS OCSO/ASD. Certifications are valid for up to two years throughout DHS. Upon expiration of certification, individuals may not derivatively classify information until they are recertified through refresher training. A waiver, not to exceed 60 days, may be granted by the Assistant Commissioner, OPR, through OPR/SMD, depending upon operational circumstances.

Personnel may be required to complete remedial training and recertification and/or may have their derivative classification authority revoked by the Assistant Commissioner, OPR, for failure to properly protect classified information resulting in a security infraction or violation.

2.17.2. Use of Personal Identifiers

CBP employees who have been appropriately trained and certified as derivative classifiers may use a personal identifier in lieu of their name and position on derivatively classified documents they create. Personal identifiers are made up of a series of numbers and letters and are unique to each individual. Personal identifiers are generated through the Integrated Security Management System (ISMS) and will be provided to derivative classifiers upon successful completion of the required training.

2.17.3. Derivative Classification Applications

When applying derivative classification markings:

(a) Classification markings cited on the source or in a security classification guide must be respected and carried forward to the newly created document.

(b) All applicable classification markings, declassification instructions, handling instructions, and the identity of the derivative classifier (by name and position or by personal identifier) must be placed on the newly created material.

(c) Markings must be applied according to the requirements of E.O. 13526, 32 C.F.R. § 2001, and the guidance provided in the ISOO booklet, *Marking Classified National Security Information*. These requirements and any supplemental markings must be implemented in accordance with Chapter 3 of this handbook and current CAPCO standards.

(d) Questions on the classification markings as they appear on the source or in a security classification guide must be referred to the originator. Refer to section 2.15 of this handbook for information regarding classification challenges.

(e) If practical, where classified information constitutes a small portion of an otherwise unclassified document, the derivative classifier must use a classified addenda or prepare a product in unclassified form to allow for maximum dissemination.

Questions about derivative classification markings may be addressed to OPR/SMD or to the appropriate Designated Security Officer for coordination with OPR/SMD.

2.17.4. Records of Derivative Classification Actions

Personnel performing derivative classification must maintain a record of each action taken. For derivatively classified documents, the record must include the total number of documents derivatively classified, by classification level.

Records of derivative classification actions are counted and reported by document, not by page. In addition, each document must be counted by its overall classification level. For example, a newly created derivatively classified document consisting of multiple pages and containing both Secret and Confidential information is counted and reported as one derivatively classified document at the Secret level.

OPR/SMD collects the required information for CBP's respective areas based on guidance provided by DHS OCSO. OPR/SMD submits one component report to DHS OCSO as part of the annual reporting requirements defined in DHS Instruction 121-01-011. As required by E.O. 13526, DHS combines the input of all components into a single DHS report using the Standard Form (SF) 311 (Agency Security Classification Management Program Data). DHS submits the completed SF-311 to ISOO as a report of the classification activity that occurred within the agency during the preceding fiscal year.

2.18. Declassification

In accordance with DHS policy, information will remain classified as long as it is in the best interest of the national security to keep it protected and the information continues to meet the classification requirements of E.O. 13526. CBP classified information, to include legacy U.S. Customs Service and U.S. Immigration and Naturalization Service information, must be declassified as soon as it no longer meets the standards for classification under E.O. 13526.

Before reviewing classified records for declassification, CBP personnel must coordinate with the CBP Records Manager to ensure that appropriate procedures are established for maintaining the integrity of the records and to ensure that NARA receives accurate information about CBP declassification actions when records are transferred to NARA.

CBP personnel who have reason to believe that the public interest in disclosure of information outweighs the need for continued classification must refer the matter to OPR/SMD. OPR/SMD will further coordinate with the appropriate OCA or the DHS Chief Security Officer for an assessment and determination on whether declassification is appropriate.

None of the provisions cited in this chapter apply to information classified in accordance with the Atomic Energy Act of 1954, as amended (RD/FRD), or North Atlantic Treaty Organization (NATO) classified information.

2.18.1. Declassification Authority

Information may be declassified or downgraded by:

(a) The Secretary of Homeland Security;

(b) The DHS Chief Security Officer;

(c) The official who authorized the original classification if that official is still serving in the same position and has original classification authority, his or her current

successor in function provided the successor is a delegated OCA, or a supervisory official of either provided the official is a delegated OCA; and

(d) CBP declassification authorities delegated in writing by the Secretary or the DHS Chief Security Officer.

i. The authority to declassify or downgrade information extends only to information for which the official has classification, program, or functional responsibility.

ii. CBP officials with declassification authority must develop and issue declassification guides, at the request and approval of ISCAP, to facilitate effective review and declassification of CBP information (which includes legacy U.S. Customs Service and U.S. Immigration and Naturalization Service information) not previously covered by a classification or declassification guide, and for information exempt from automatic declassification.

iii. Declassification authority is not required for simply canceling or changing classification markings in accordance with declassification or downgrading instructions cited on a document, directions found in a security classification guide or declassification guide, or instructions received from an OCA or declassification authority.

Classified information that has been declassified without proper authority, as determined by an OCA with jurisdiction over the information, remains classified, and administrative action must be taken to restore markings and controls, as appropriate. All such instances must be reported to DHS OCSO/ASD for notification to ISOO.

2.18.2. Extension of Classification

If an OCA with jurisdiction over the information does not extend the classification of information that has been assigned a specific date or event for declassification, and the information does not contain classified equities of another agency, the information is automatically declassified upon the occurrence of the date or event.

If an OCA has assigned a date or event for declassification that is less than 25 years from the date of origin, an OCA with jurisdiction over the information may extend the classification duration of such information for a period not to exceed 25 years from the date of classification.

Decisions to extend classification must take into account the potential difficulty of notifying holders of the extension, including the possible inability to ensure continued, uniform protection of the information. Officials who make a determination to extend a declassification date are responsible for notifying holders of the information of the decision and for providing a new date and instructions for declassification.

2.18.3. Automatic Declassification of Permanent Historical Records

E.O. 13526 mandates that information contained within permanently valuable historical records (as defined by Title 44, U.S.C.) be automatically declassified 25 years from the date of origin of the document. All classified records are automatically declassified on December 31 of the year that is 25 years from the date of origin, except where such information has been exempted from automatic declassification at 25 years.

2.18.4. Exemption from Automatic Declassification

(a) Information not contained in a file series

The Secretary or the DHS Chief Security Officer may propose to exempt specific information not otherwise contained in an exempted file series from automatic declassification. Such information may be exempted from automatic declassification only if its release could be expected to:

i. Reveal the identity of a confidential human source or a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;

ii. Reveal information that would assist in the development, production, or use of weapons of mass destruction;

iii. Reveal information that would impair U.S. cryptologic systems or activities;

iv. Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

v. Reveal 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;

vi. Reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

vii. Reveal information that would seriously impair the current ability of U.S. government officials to protect the President, Vice President, and other individuals for whom protection services, in the interest of the national security, are authorized;

viii. 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; or

ix. Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

Proposed exemptions from automatic declassification at 25 years are identified through the creation of a declassification guide. For CBP information that falls within one or more of the categories identified above, exemption requests must be endorsed by the Commissioner and submitted, in the form of a declassification guide, to DHS OCSO/ASD. DHS OCSO/ASD verifies that the proposed declassification guide and its exemptions meet the standards of E.O. 13526 and, upon concurrence, processes the guide through ISOO and the ISCAP.

(b) Information contained in a specific file series

Specific file series may be exempt from the 25-year automatic declassification provisions of E.O. 13526. Such exemption requests are processed in the same

manner as section (a) above. In addition, submissions to DHS OCSO/ASD must include:

i. A description of the file series; and

ii. 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.

Information exempted from automatic declassification at 25 years remains subject to the mandatory and systematic declassification review provisions of E.O. 13526. Information exempted from automatic declassification through a file series exemption is still subject to mandatory declassification review. Copies of records from an exempted file series located elsewhere are not exempt from automatic declassification.

2.18.5. Onset of Automatic Declassification

The following provisions apply to the onset of automatic declassification:

(a) Classified records within an integral file block that are otherwise subject to automatic declassification are not automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(b) In consultation with the Director of the National Declassification Center, before the records are subject to automatic declassification, the Secretary or the DHS Chief Security Officer may delay automatic declassification for up to five additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly.

(c) By notification to the Director, ISOO, the Secretary or DHS Chief Security Officer may delay automatic declassification for up to 90 days from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

2.18.6. Mandatory Declassification Reviews

Individuals, to include U.S. citizens, legal permanent residents, foreign government entities, or representatives thereof, may request a review for declassification of information classified under E.O. 13526, or its predecessor orders. Such requests are sent to the Department of Homeland Security, Director, Departmental Disclosure, Privacy Office, Washington, DC 20528.

Information originated by the incumbent President; the incumbent President's White House Staff; committees, commissions, or boards appointed by the incumbent President; or other entities within the Executive Office of the President that solely advise and assist the incumbent President are exempt from the provisions of this section.

(a) <u>Responsibilities</u>

The DHS Disclosure Office serves as the central processing point for all mandatory review requests concerning DHS information. The Disclosure Officer will promptly,

but no later than 30 days after receipt, forward mandatory review requests to CBP if CBP has primary jurisdiction over the requested information. The Disclosure Officer will provide the requester with an acknowledgment of receipt of the request.

CBP will promptly process requests received from the DHS Disclosure Office. The CBP Privacy and Diversity Office, Freedom of Information Act (FOIA) Division, receives such requests and coordinates reviews of the requested information with OPR/SMD. Information reviewed will be declassified if it no longer meets the standards for classification established by E.O. 13526. Information that is declassified will be released to the requester unless withholding is appropriate under applicable law (e.g., the FOIA or the Privacy Act of 1974).

(b) Mandatory Review Requests

Requests must describe the information or material with enough specificity to allow it to be located with a reasonable amount of effort. When the description of the information in the request is deficient, the CBP FOIA Office will solicit as much additional identifying information as possible from the requester. If the information or material requested cannot be obtained with a reasonable amount of effort, the CBP FOIA Office will provide the requester, through the DHS Disclosure Office, with written notification of the reasons why no action will be taken and of the requester's right to appeal.

Requests for review of information that has been subjected to a declassification review request within the preceding two years will not be processed. The Disclosure Officer will notify the requester of such denial.

Requests for information exempted from search or review under sections 701, 702, or 703 of the National Security Act of 1947 (50 U.S.C. § 3141, 3142, and 3143), will not be processed. The Disclosure Officer will notify the requester of such denial.

If documents or materials being reviewed for declassification contain information that has been originally classified by another government agency, the reviewing activity will notify the Disclosure Officer, who refers the matter to the originating agency. Unless the association of that organization with the requested information is itself classified, the Disclosure Officer will then notify the requester of the referral.

CBP will refuse to confirm or deny the existence, or non-existence, of requested information when the fact of its existence, or non-existence, is properly classified.

CBP will make a final determination on requests received as soon as practicable, but within one year of receipt. When information cannot be declassified in its entirety, CBP will make reasonable efforts to redact the portions that still meet the standards for classification and release the declassified portions of the requested information that constitute a coherent segment. Withheld portions must be marked to indicate the authority for such.

CBP will notify the Disclosure Officer of the determination made in the processing of a mandatory review request. Notifications must include the number of pages declassified in full, the number of pages declassified in part, and the number of pages where declassification was denied.

The Disclosure Officer will maintain a record of all mandatory review actions for reporting in accordance with applicable Federal requirements.

(c) Appeals

The mandatory declassification review system provides for administrative appeal in cases where the review results in the information remaining classified. The requester will be notified of the results of the review and of the right to appeal the denial of declassification. To address such appeals, the DHS Disclosure Office will convene a DHS Classification Appeals Panel (DHS/CAP). At a minimum, the DHS/CAP consists of representatives from the DHS Disclosure Office, DHS OCSO, the DHS Office of General Counsel, and a representative from CBP, if CBP has jurisdiction over information involved.

If the requester files an appeal through the DHS/CAP and the appeal is denied, the requester will be notified of the right to appeal the denial to ISCAP.

2.18.7. FOIA and Privacy Act Requests

If a requester submits a request under both the mandatory declassification review provisions cited in this handbook and 5 U.S.C. § 552 (Freedom of Information Act), the requester will be advised 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.

2.18.8. Systematic Declassification Reviews

CBP conducts systematic declassification reviews for classified information that is exempted from automatic declassification and:

(a) Has been identified as a priority by the National Declassification Center;

(b) Contains information that has been identified to have significant value for historical or scientific research or for promoting the public welfare; and

(c) Has a reasonable likelihood of being declassified upon review.

CBP personnel may contact OPR/SMD for further guidance on systematic declassification reviews.

2.18.9. Downgrading

Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level and can be properly protected at a lower level. Information must be downgraded by an official authorized to originally classify the information.

(a) Existing documents that identify a specific date or event when the information is to be downgraded are downgraded automatically upon occurrence of that date or event, unless they have been reviewed and the classification status has been changed by an OCA.

(b) Downgrading Decisions During Original Classification

Downgrading must be considered when original classifiers are deciding on the duration of the classification to be assigned. If downgrading dates or events can be identified, the dates or events are specified along with the declassification instruction. Downgrading instructions do not replace declassification instructions.

(c) Downgrading at a Later Date

Information may be downgraded by the Secretary, the DHS Chief Security Officer, the official who authorized the original classification if that official is still serving in the same position and has original classification authority, his or her current successor in function provided the successor is a delegated OCA, or a supervisory official of either provided the official is a delegated OCA.

2.19. Restricted Data/Formerly Restricted Data

CBP personnel who access and/or generate RD/FRD must comply with the requirements of 10 C.F.R. § 1045 (Nuclear Classification and Declassification) and DHS implementing guidance. For comprehensive guidance on the proper safeguarding and handling of RD/FRD, refer to DHS Instruction 121-01-011, Chapter 6 (Restricted Data and Formerly Restricted Data).

2.20. Foreign Government Information

Information classified by a foreign government is generally treated the same as its U.S. equivalent. Unless otherwise subject to statute, treaty, or other international agreement, CBP personnel who handle classified foreign government information must do so in accordance with DHS Instruction 121-01-011, Chapter 8 (Classified Foreign Government Information).

3. Marking Classified Information

A uniform security classification system requires that standard markings be applied to classified information. At the time of original classification, all national security information must be marked in a manner appropriate to the medium involved. Markings must be applied according to the requirements of E.O. 13526, 32 C.F.R. § 2001, and the guidance provided in the Information Security Oversight Office (ISOO) booklet, *Marking Classified National Security Information*.

The ISOO booklet, *Marking Classified National Security Information*, establishes the uniform security classification system for standard markings that are applied to originally or derivatively classified information. For additional information, see DHS Instruction 121-01-011, Chapter 9 (Marking).

3.1. Overall and Portion Markings

The following are applicable to all classified documents:

(a) The cover, first page, and title page (if any) must be prominently marked at the top and bottom of the page with the highest classification of information contained within the document.

(b) Either the highest classification of information in the document or on the page must be prominently marked at the top and bottom of every page.

(c) A classification block must be located so that it is immediately apparent on the cover page or first page. The classification block must indicate the person who created the document along with his or her title and office or personal identifier, the basis for the classification, and a declassification instruction.

(d) Each paragraph, sub-paragraph, subject line, title, graphic, table, chart, bullet statement, classified signature block, picture, or other portion of a document (to include information presented in slide format) must be portion marked to indicate the highest level of classification in the marked portion.

(e) Portion markings are (TS) for Top Secret, (S) for Secret, (C) for Confidential, and (U) for Unclassified.

(f) The date of the document must be readily apparent.

(g) When marking documents that are classified by compilation, any unclassified portions must be portion marked "(U)," while the overall markings reflect the classification of the compiled information, even if all the portions are marked "(U)." In such situations, clear instructions must appear with the complied information to indicate when individual portions constitute a classified compilation and when the individual portions do not.

3.2. Original Classification Markings

At the time of original classification, the following information must appear on the face of each classified document or be applied to other classified media in an appropriate manner:

(a) Classified By: This line indicates the identity (by name or personal identifier) and position of the original classification authority, and the agency and office of origin, if not otherwise evident;

(b) Reason: This line identifies the reason for classification as provided in E.O. 13526, Section 1.4 (e.g., 1.4(g)); and

(c) Declassify On: This line indicates the duration of classification, determined by one of the following declassification instructions:

i. A date or event for declassification that corresponds to the lapse of the information's national security sensitivity, which is equal to or less than 10 years from the date of the original classification decision;

ii. A date not to exceed 25 years from the date of the original classification decision. When displayed numerically, the following format is used: YYYYMMDD. Spelling out or abbreviating the month (e.g., January 1, 2015 or Jan 1, 2015) is also acceptable;

iii. If the classified information is clearly and demonstrably expected to reveal the identity of a confidential human source or a human intelligence source, the marking "50X1-HUM" is used and no date or event is annotated; or

iv. If the classified information is clearly and demonstrably expected to reveal key design concepts of weapons of mass destruction, the marking "50X2-WMD" is used and no date or event is annotated.

Example of original classification block:

Classified By: *Name, position, and office*
Reason: *Applicable reason as cited in E.O. 13526, Section 1.4 (e.g., 1.4(g))*
Declassify On: *Date or event not to exceed 25 years (e.g., 20360404)*

3.3. Derivative Classification Markings

At the time of derivative classification, the following information must appear on the face of each classified document or be applied to other classified media in an appropriate manner:

(a) Classified By: This line indicates the identity (by name or personal identifier) and position of the derivative classifier and the office of origin;

(b) Derived From: This line indicates the source documents or classification guide used. If the document is derived from multiple sources, this is indicated in the "Derived From" line, and a listing of the classified sources is included in, or attached to, the document. If a document is derived from a single source that is itself derived from multiple sources, the title of the source, not multiple sources is indicated in the "Derived From" line; and

(c) Declassify On: This line indicates the date or event as identified on the source document. When using multiple sources, the declassification instruction applied must be the most restrictive declassification date or event from the sources. When displayed numerically, the following format is used: YYYYMMDD. Spelling out or abbreviating the month (e.g., January 1, 2015 or Jan 1, 2015) is also acceptable.

Example of derivative classification block:

Classified By: *Name, position, and office of origin (if not otherwise evident) or personal identifier*
Derived From: *Identity of source document(s)*
Declassify On: *Date or event as reflected on the source*

When a document is derivatively classified from a source document or a classification guide in which the declassification instruction is "Originating Agency's Determination Required" (OADR), "Manual Review" (MR), or any of the exemption markings (X1 through X8), the derivative classifier must calculate a date that is 25 years from the date of the source document to determine the derivative document's declassification date or event. In addition, "Director of National Intelligence Only" (DNI Only), "Director of Central Intelligence Only" (DCI Only), and "Subject to Treaty or International Agreement" are no longer authorized for use in the "Declassify On" line.

3.4. Working Papers

Working papers are documents or materials, regardless of media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers containing classified information must be dated when created, marked with the highest classification of any information contained in each document, protected at that level, and, if appropriate, destroyed when no longer needed. Working papers must be controlled and marked in the same manner prescribed for a finished document at the same classification level in the event the document is:

(a) Released outside of the originating office or activity;

(b) Retained for more than 180 days from the date of origin; or

(c) Filed permanently.

3.5. Transmittal Documents

A transmittal document must indicate on its face the highest classification level of any classified information attached or enclosed. The transmittal document must also include the following or similar instructions, as appropriate: "Unclassified when classified enclosure removed," or, if the transmittal document itself contains classified information, "Upon removal of attachments, this document is (*classification level*)."

3.6. Other Materials

Bulky material, equipment, and facilities must be identified clearly in a manner that leaves no doubt about the classification status, the level of protection required, or the duration of classification. If identification itself would reveal classified information (such

as a covert facility), such identification is not required; however, documentation of such must be maintained by the Office of Professional Responsibility, Security Management Division.

3.7. Declassification Markings

Declassified materials must be marked "DECLASSIFIED." All classification markings such as headers, footers, and portion markings must be lined through. The front page must identify by name and position or personal identifier the authority for declassification as cited in section 2.18.1 of this handbook, and where applicable, a declassification guide identified by title and date.

3.8. Email Messages

Email messages transmitted on or prepared for transmission on classified systems or networks must be configured to display the overall classification level at the top and bottom of the body of the message. The overall classification marking string for the email must reflect the classification of the header and body of the message. This includes the subject line, the text of the email, a classified signature block, attachments, included messages, and any other information conveyed in the body of the email. A single linear text string showing the overall classification and markings must be included in the first line of text and at the end of the body of the message after the signature block.

Classified email messages must be portion marked. Each portion must be marked to reflect the highest level of information contained in that portion. A text portion containing a URL or reference (i.e., link) to another document must be portion marked based on the classification of the content of the URL or link text, even if the content to which it points reflects a higher classification marking.

Subject lines must be portion marked to reflect the sensitivity of the information in the subject line itself and do not reflect any classification markings for the email contents or attachments. Subject lines and titles must be portion marked before the subject or title.

A classified signature block must be portion marked to reflect the highest classification level of the information contained in the signature block itself. The classification authority block is placed after the signature block, but before the overall classification marking string at the end of the email. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

When forwarding or replying to an email, personnel must ensure that, in addition to the markings required for the content of the reply or the forwarded email itself, the markings reflect the overall classification and declassification instructions for the entire string of emails and attachments. This includes any newly drafted material, material received from previous senders, and any attachments.

When files are attached to another electronic message or document, the overall classification of the message or document accounts for the classification level of the attachment and the message or document is marked to indicate the classification of the email without the attachment.

For more information on marking classified information in electronic formats, refer to DHS Instruction 121-01-011, Chapter 9 (Marking).

4. Access and Dissemination

Federal employees are not automatically granted access to classified information. An employee is eligible for access to classified information only when the employee has been determined to be trustworthy by an appropriate background investigation and when access is essential to the accomplishment of lawful and authorized government purposes.

4.1. Access and Dissemination Restrictions

Classified information may be discussed and disclosed under the following conditions:

(a) The recipient of the classified information has a current security clearance at the appropriate level, and the security clearance has been verified in accordance with the CBP Personnel Security Handbook, HB 1400-07A.

(b) The holder of the classified information has validated that the recipient's need to know is in the performance of official government duties and the mission needs of the organization to which he or she is assigned.

(c) The recipient has the means to protect, store, or destroy the information in accordance with E.O. 13526 and other applicable DHS and CBP policies.

4.2. Access to Classified Information

Access to classified information is limited to persons whose official duties require knowledge or possession of the information. No individual has a right to access classified information solely by virtue of office, rank, or position.

Before classified information is disclosed, the holder must verify the recipient's security clearance through the Office of Professional Responsibility (OPR), Personnel Security Division (PSD); the Designated Security Officer (DSO); or other CBP personnel who have been authorized by OPR/PSD to verify personnel security clearances through CBP's official security clearance database. (Note: The numerical security clearance indicator that appears on some Personal Identity Verification (PIV) cards is not an authorized means of validating an individual's security clearance. The indicator reflects the cardholder's security clearance level at the time of the card's issuance and may not reflect the individual's current clearance status.)

4.2.1. Personnel Security Clearances

When an employee's security clearance has been approved, OPR/PSD notifies the individual's supervisor by email and provides the forms to be signed by the employee. Employees who are granted security clearances receive a briefing on the safeguarding and handling of classified information and must sign the SF-312 (Classified Information Nondisclosure Agreement) and the Reporting Foreign Contacts form. The signed forms must be submitted to OPR/PSD prior to formally granting a security clearance.

When an employee no longer requires a security clearance due to a change in duties/responsibilities, transfer, resignation, or retirement, the security clearance must be administratively terminated. Prior to termination of a security clearance, the employee must receive a formal security debriefing describing his or her continuing responsibility to protect the classified national security information to which he or she had access. The security debriefing is provided by the employee's supervisor, the DSO, the OPR Security

Management Division (SMD), or other designated personnel. The Security Debriefing Acknowledgement portion of the SF-312 must be signed by the employee, witnessed by the official who provided the debriefing, and sent to OPR/PSD along with a request to terminate the clearance. OPR/PSD updates CBP records to reflect the termination.

4.2.2. Contractors and Consultants

As defined in the National Industrial Security Program Operating Manual (NISPOM), contractors and consultants working in the Federal Government must not be given access to classified material without the execution of a classified contract and DD Form 254 (Contract Security Classification Specification), unless they are tied to a contract in which a DD Form 254 has been executed. For more information on classified contracts and DD Form 254 processing, refer to Chapter 9 of this handbook.

Contractors and consultants may be granted access to classified material in the custody of CBP after meeting the requirements identified above and after the Contracting Officer's Representative has verified the applicable contractors hold the appropriate security clearance through the Defense Security Service.

As defined in the CBP Personnel Security Handbook, HB 1400-07A, contractors and consultants are required to undergo background investigations to determine suitability for employment with CBP. CBP offices that require contractors and/or consultants to access classified information are required to comply with E.O. 12829 and the NISPOM.

4.2.3. Visitors

(a) CBP Visitor Certifications

CBP employees who have a need to verify their security clearance status with another government agency or contracting facility must initiate CBP Form 6101 (Classified Visit Authorization Request), in accordance with the CBP Personnel Security Handbook, HB 1400-07A. Some agencies or government facilities require the use of their own form for visits to their facilities. The individual coordinating the security clearance certification must verify the method acceptable to other agencies prior to the visit.

(b) Non-CBP Visitor Certifications

For non-CBP personnel visiting CBP facilities for meetings or projects in which classified information is shared, the employing agency or contractor facility must provide certification of the individual's security clearance to the CBP office to be visited. CBP personnel must not disclose any classified information to a visitor until notified that the visitor's security clearance has been verified.

4.2.4. Access by Persons Outside of the Executive Branch

Classified information may be made available to individuals or agencies outside the Executive Branch provided the requirements in section 4.1 of this handbook are met.

(a) Judicial Branch

CBP personnel receiving a litigation request or a demand for official CBP information or testimony concerning such information must immediately notify the CBP Office of

the Chief Counsel (OCC) or servicing regional Associate or Assistant Chief Counsel. OCC will consult with the DHS Office of the General Counsel accordingly for all requests. Classified information entered into the Judicial System must be handled in accordance with the Classified Information Procedures Act (Public Law 96-456). Justices of the U.S. Supreme Court and judges of the U.S. Courts of Appeals and district courts do not require an investigation and determination of eligibility for access to classified information. All other members of the Judiciary who require access to classified information must be appropriately investigated and granted security clearances.

(b) Congress

Access to classified information or material by Congress, its committees, members, and staff representatives must be coordinated with the CBP Office of Congressional Affairs. The Office of Congressional Affairs will further coordinate with the DHS Office of Legislative Affairs. Any CBP employee testifying before a congressional committee in executive session, in relation to a classified matter, must first obtain the assurance of the committee that individuals present have security clearances commensurate with the highest classification of information that may be discussed. Members of Congress, by virtue of their elected positions, do not require an investigation and determination of eligibility for access to classified information. All other congressional staff members and other associated officials who require access to classified information must be appropriately investigated and granted security clearances. (The Office of Inspector General is exempt from this requirement when acting in official capacity.)

(c) State, Local, Tribal, and Private Sector (SLTPS) Officials

Access to classified information by SLTPS officials must be consistent with the standards and requirements for access by executive branch personnel as cited in E.O. 13549 and its implementing directives.

(d) Foreign Nationals

U.S. intelligence information and other classified information may be shared with foreign nationals only when consistent with U.S. national security and foreign policy objectives and when an identifiable benefit can be expected for the United States. To share such information with foreign nationals and perform relevant security clearance verifications, contact the CBP Office of Intelligence (OI), which further coordinates with the DHS Foreign Disclosure Office.

(e) Representatives of the Government Accountability Office (GAO)

Representatives of GAO may be granted access to classified information when such information is relevant to the performance of the statutory responsibilities of that office. Certifications of security clearances, and the basis thereof, is accomplished pursuant to arrangements between GAO and CBP.

(f) Government Printing Office (GPO)

Documents and material of all classification levels may be processed by GPO, which protects the information in accordance with the guidelines outlined in E.O. 13526.

(g) Historical Researchers

Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that a CBP original classification authority (OCA) with classification jurisdiction over the information accomplishes the following:

i. Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted, and certifies that the researcher has been found to be trustworthy based on such investigation as determined by the DHS Chief Security Officer;

ii. Limits such access to specific categories of information over which CBP has classification jurisdiction, and to any other category of information for which the researcher obtains the written consent of another DHS OCA or non-DHS department or agency that has classification jurisdiction over information contained in or revealed by the document, within the scope of the proposed historical research;

iii. Maintains custody of the classified material at a DHS installation or activity, or authorizes access to documents in the custody of the National Archives and Records Administration (NARA);

iv. Obtains the researcher's agreement to safeguard the information and to submit any notes and manuscripts for review by CBP, DHS, or non-DHS departments or agencies with classification jurisdiction for a determination that no classified information is contained therein. These requirements must be included in a nondisclosure agreement, which is to be executed by the researcher as a condition of access; and

v. Issues an authorization for access valid for not more than two years from the date of issuance.

(h) Former Political Appointees

Former political appointees may be authorized access to information they originally classified while in their position provided that a CBP OCA with current classification jurisdiction over the information accomplishes the following:

i. Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted, and certifies that the former appointee has been found to be trustworthy based on such investigation as determined by the DHS Chief Security Officer;

ii. Limits such access to specific categories of information over which CBP has classification jurisdiction, and to any other category of information for which the former appointee obtains the written consent of another DHS OCA or non-DHS department or agency that has classification jurisdiction over information contained in or revealed by the document, within the scope of the proposed access;

iii. Maintains custody of the classified material at a DHS installation or activity, or authorizes access to documents in the custody of NARA; and

iv. Obtains the former political appointee's agreement, through the execution of a nondisclosure agreement, to safeguard the information and to submit any notes and manuscripts for review by CBP, DHS, or non-DHS departments or agencies with classification jurisdiction for a determination that no classified information is contained therein.

4.2.5. Protected Disclosures

For information regarding protected disclosures as defined by Presidential Policy Directive 19, *Protecting Whistleblowers with Access to Classified Information*, refer to DHS Instruction 121-01-007-01, *Personnel Security, Suitability and Fitness Program*.

4.3. Dissemination of Classified Information

4.3.1. Other Agency Information

Classified information originating in one agency may be disseminated to another agency or a state, local, tribal, or private sector entity without the consent of the originating agency, as long as the criteria for access are met. The exception to this is if the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information, in accordance with E.O. 13526 and its implementing directives. In the case of classified information related to intelligence sources, methods, and activities, the Director of National Intelligence determines when such prior authorization is required.

Documents created prior to June 28, 2010, must not be disseminated outside any other agency to which they have been made available without the consent of the originating agency.

4.3.2. Emergency Situations

The Secretary of Homeland Security has delegated the Commissioner and the Assistant Commissioner, OI, the authority to disclose classified information to otherwise unauthorized individuals in emergencies and when necessary to respond to an imminent threat to life or in defense of the homeland. This authority is delegated under the provisions of DHS Delegation 12000, *Delegation for Security Operations within the Department of Homeland Security, Appendix 1 – Designated Officials*. Under these conditions, the approving official:

(a) Limits the amount of classified information disclosed and the number of individuals to whom it is disclosed to the absolute minimum necessary to achieve the intended purpose;

(b) Transmits the classified information via approved Federal government channels by the most secure and expeditious method possible, or by other means necessary when time is of the essence;

(c) Provides instructions about what specific information is classified and how it must be safeguarded. Physical custody of classified information remains with an authorized

Federal government entity in all but the most extraordinary and unique circumstances;

(d) Provides appropriate briefings to the recipients on their responsibilities not to disclose the information and obtains signed nondisclosure agreements. In emergency situations requiring immediate verbal release of information, the signed nondisclosure agreement memorializing the briefing may be received after the emergency abates;

(e) Within 72 hours of the disclosure of classified information, or at the earliest opportunity that the emergency permits but no later than seven days after the release, the disclosing authority notifies the DHS Office of the Chief Security Officer (OCSO), Administrative Security Division (ASD), and the originating agency of the information. The notification includes:

i. A description of the disclosed information;

ii. To whom the information was disclosed;

iii. How the information was disclosed and transmitted;

iv. Reason for the emergency release;

v. How the information is being safeguarded; and

vi. A description of the briefings provided and a copy of the nondisclosure agreements signed.

Copies of the signed nondisclosure agreements must be forwarded with the notification or as soon thereafter as practical. Release of information pursuant to this authority does not constitute declassification thereof. This authority may not be further delegated.

4.3.3. Classified Meetings and Conferences

(a) Meetings and conferences that involve classified information present vulnerabilities for unauthorized disclosure, and therefore require prior approval and coordination with DHS OCSO/ASD through OPR/SMD. The dissemination of classified information to large audiences increases security risks and may involve substantial costs to provide adequate security. Large meetings involving the dissemination of classified information will only be authorized when the head of the host office determines the following in writing:

i. The meeting serves a specific Federal government purpose.

ii. The use of other prescribed channels for dissemination of classified information or material is insufficient.

iii. The meeting location is in the space of and under the security control of a Federal government agency or a U.S. contractor with an appropriate facility security clearance.

iv. The meeting is not held in commercial space (e.g., hotel conference facilities) without prior approval.

v. Adequate security procedures have been developed and implemented to minimize risk to the classified information involved, as described in section (b) below.

vi. Classified sessions are segregated from unclassified sessions whenever possible.

vii. Access to the meeting or conference, or specific classified sessions thereof, is limited to persons who possess an appropriate security clearance and need to know.

viii. Valid government-issued identification is used to verify the identity of attendees.

ix. Announcement of the classified meeting is limited to a general description of the topics to be presented, names of speakers, logistical information, and administrative and security instructions. Non-government organizations may assist in organizing and providing administrative support for a classified meeting, but all security requirements remain the specific responsibility of the CBP office sponsoring the meeting. Procedures ensure that classified documents, recordings, audiovisual material, magnetic media, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as required by other provisions of this Instruction. Note taking or electronic recording during classified sessions is permitted only when it is determined that such action is necessary to fulfill the Federal government purpose for the meeting and accommodations are made to ensure materials are properly secured and transported.

x. The CBP office sponsoring the meeting must appoint a CBP official to serve as the security manager for the meeting.

xi. Other Federal government organizations or cleared U.S. contractors with appropriate facility security clearances may assist with implementing security requirements under the direction of the appointed security manager.

xii. A physical security assessment of the selected facility and/or a Technical Surveillance Countermeasure survey is conducted if deemed necessary by OPR/SMD.

(b) For in-house gatherings and other impromptu meetings where classified information is discussed, it is incumbent upon the CBP office sponsoring the meeting to ensure appropriate security measures are in place. Those measures include:

i. The meeting is held in the space of or under the secure control of a Federal government agency or at an appropriately cleared U.S. contractor facility.

ii. All electronic equipment in the room that is capable of transmitting signals outside the room is powered off and disconnected from electrical outlets.

iii. A sound attenuation test is conducted to ensure normal conversational tone from inside the room cannot be heard intelligibly from outside the room, including vents, ducts, and other openings. If public address or other amplification systems are used, conduct the test with these systems on and off.

iv. Cleared host office personnel are stationed at exterior doors and hallways to keep the room's perimeter under surveillance and prevent passers-by from stopping and listening.

v. Access to the room is controlled and an attendee roster is used, if applicable. Sufficient backup host office personnel are available as needed.

vi. The identity of each participant is verified via U.S. government photo identification or equivalent documentation.

vii. The security clearances of attendees are equal to or higher than the level of classified information to be disclosed and have been verified in accordance with the CBP Personnel Security Handbook, HB 1400-07A, and section 4.2 of this handbook.

viii. Those without proper authorization and clearance are prohibited from attending classified portions of the meeting.

ix. The number of room entrances and other access methods is limited prior to or during the meeting to prevent access by unauthorized persons.

x. All attendees and presenters are informed in advance of the highest level of classified information to be presented/discussed. When multiple presentations are to be given, all attendees are notified of the specific classification (or unclassified status) of each presentation.

xi. Attendees are notified of limitations associated with classified portions of the meeting, including prohibitions against photographing, note taking, audio/video recording, and using two-way radios, cellular phones, or other transmitting devices.

xii. Announcements of the meeting are unclassified and do not contain descriptions of the specific classified subjects that are to be presented.

xiii. Security protection for the room is maintained during breaks.

xiv. All security safeguards for classified information are observed.

xv. At the conclusion of the meeting, an inspection of the room is conducted to ensure no classified materials have been left behind.

xvi. If applicable, and if attendees have valid courier cards, sufficient supplies are provided to properly package classified materials for local attendees to hand-carry back to their offices.

See Appendix A for additional information on conducting classified meetings and conferences.

5. Custody and Accountability

Personnel who have been granted access to classified information are responsible for protecting the information in their possession or control and for ensuring necessary precautions are taken to prevent unauthorized access.

5.1. Protection of Classified Information

The following measures must be taken to ensure proper protection of classified information:

(a) Classified information must be appropriately stored in a General Services Administration (GSA)-approved security container at all times when not in use, except in authorized circumstances, such as when stored in approved open-storage facilities.

(b) Before granting access to classified material, CBP personnel must verify the recipient's security clearance in accordance with the CBP Personnel Security Handbook, HB 1400-07A, and section 4.2 of this handbook.

(c) An office that receives classified information (in any form) and has no authorized equipment available to properly store it must return the classified material to the sender, arrange to properly store the information with another office, or destroy it by an approved method, as described in section 5.7 of this handbook.

(d) Custodians of classified information must ensure that persons who do not possess an appropriate security clearance and need to know are not able to access classified information.

(e) Classified information must be covered with the appropriate cover sheet (SF-703, *Top Secret*; SF-704, *Secret*; or SF-705, *Confidential*).

5.2. Custody during Emergencies

In the event of a fire, natural disaster, civil disturbance, terrorist event, hostile action, or unexpected and immediate evacuation of office space, classified information must be secured in a GSA-approved security container or safe or be properly destroyed.

Each CBP office that handles or stores classified material must prepare a general plan for the protection and destruction of classified information in the event of an emergency. Such plans must be forwarded to the Office of Professional Responsibility (OPR), Security Management Division (SMD) and/or the Designated Security Officer (DSO) for review and approval on an annual basis. Refer to Appendix B for a sample emergency action plan.

The plan must include the priority of safeguarding or destroying classified material, persons responsible for the safeguarding or destruction, and the recommended place and method for the safeguarding or destruction. The plan must also address what to do if there is no time or available method to properly store or destroy the information.

The classified material destruction plan must be distributed to all cleared personnel within the office storing classified information. The DSO and/or other designated

security liaisons must ensure that cleared personnel are briefed on their responsibilities defined within the plan.

5.3. Designated Security Officer and Classified Document Custodian

In order to control and account for classified information, each CBP program office, sector, field office, and air and marine location must designate a DSO, as described in section 1.4.9 of this handbook. The DSO is the point of contact for security-related questions, issues, and inspections and serves as an intermediary between the office and OPR/SMD. See Appendix C for information regarding the roles and responsibilities of the DSO.

Where classified information is stored, a Classified Document Custodian (CDC), as described in section 1.4.10 of this handbook, must be appointed. The CDC is responsible for security containers within his or her respective office space, including combinations, document control, and container forms. Refer to Appendix D for more information about the responsibilities of the CDC.

CBP personnel who are designated in these roles ensure that the movement of classified information can be traced, dissemination is limited, prompt retrieval of information can be achieved, the loss of information can be detected, and excessive holding and reproduction of information is limited. However, personnel who serve as DSOs and CDCs are not personally accountable for the actions of other CBP personnel who are authorized to handle classified information.

Classified information (in any form), to include extra copies, is not personal property and must not be removed from DHS control by any departing employee, contractor, or consultant. The DSO and other designated security liaisons must ensure that debriefed personnel account for all classified information in their possession and transfer it to an authorized custodian prior to their departure from CBP.

5.4. Accountability of Classified Information

Within CBP, each program office that handles and stores classified information is required to conduct an inventory of all classified holdings stored within its security container(s) by September 30 of every year (once each fiscal year). The annual inventory will be conducted by the office's designated CDC under the oversight of the appointed DSO. For additional information on annual security container inventories, refer to section 6.11 of this handbook.

Assistant Commissioners; the Chief, U.S. Border Patrol; and directors may require the use of additional accountability records within their respective offices at their discretion.

5.5. Receipts for Classified Information Transmission

When transportation or transmission of classified information occurs outside of a CBP office or facility, the custodian of the information is responsible for its proper transmission. For additional information on escorting and hand-carrying classified materials, refer to section 7.4 of this handbook.

5.5.1. Top Secret and Secret

Receipts for Top Secret and Secret classified information transmitted or transferred outside of CBP are required and must be returned to the transmitting office within 30 days of receipt. DHS Form 11000-11 (Record of Transmittal for Classified Documents or Other Accountable Material) is used for this purpose. The CDC or the sender who transmits the classified information must maintain a suspense copy of all document receipts for classified material transferred external to CBP. If a signed receipt is not received within 30 days from the entity to which the classified information was transmitted, a follow-up receipt must be mailed to the entity that received the information. If a signed receipt is still not received within two more weeks, the sender or CDC must contact the recipient organization to determine the status of the classified material.

5.5.2. Confidential

With the exception of certain categories of information (e.g., North Atlantic Treaty Organization (NATO) information, foreign government information, and materials transmitted to a cleared contractor), receipts for Confidential materials are at the discretion of the sender.

5.6. Reproduction of Classified Material

Documents and other material containing classified information must be reproduced only when necessary to accomplish the mission of the organization or for compliance with applicable statutes or directives. Security measures must be in place to prevent unauthorized individuals from gaining access to copies of classified information, the misuse of copiers by authorized personnel, and information retention through latent or residual images on the machines or in their electronic memories.

The use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is recommended. OPR/SMD, in coordination with the Office of Information and Technology or the Information Systems Security Officer, can provide guidance in determining if a copier meets the proper requirements for reproduction of classified information.

5.6.1. Control Procedures

The following control procedures must be in place when reproducing classified material:

(a) Reproduction must be kept to a minimum consistent with mission requirements.

(b) Classified material must not be reproduced on equipment that poses unacceptable risks (e.g., machines that are connected to an unclassified local area network (LAN) or are equipped with remote diagnostics or an internal memory, or in some other way retain images).

(c) Personnel who reproduce classified material must be aware of the risks involved with specific reproduction equipment and the appropriate countermeasures they are required to take.

(d) Reproduced material must be clearly identified as classified at the applicable level.

(e) Reproduced material must be placed under the same accountability and control requirements that apply to the original material.

(f) Waste products generated during reproduction must be properly protected and disposed of.

5.6.2. Copier Requirements

Machines with unacceptable risks, such as machines that are connected to an unclassified LAN, equipped with remote diagnostics, equipped with an internal memory, or otherwise able to retain images, are not approved for classified reproduction.

Approved machines must be located in locked or secure areas to prevent access by unauthorized users. If no locked or secure area is available, the copier must be located away from high-traffic areas where unauthorized persons are situated. The location must allow continuous monitoring of the copier by office personnel during work hours.

After a copier is designated "approved," it must be affixed with an SF label (SF-706, Top Secret; SF-707, Secret; or SF-708, Confidential) to indicate the classification level it is approved to copy. Copiers in the same immediate area that are not approved for classified information must display SF-710 (Unclassified) labels to serve as a reminder not to copy classified information on those machines. If a facility does not have any copiers approved for classified copying, the use of SF-710 labels is recommended but not required.

5.6.3. Copier Security Procedures

Reproduction of classified information must be done using an approved copier machine, as defined in section 5.6.2 of this handbook. Cleared individuals must remain at the copier until classified reproduction is complete. Before leaving the copier, cleared individuals must check the copier for any copies or originals that may be left in or around the copier.

Additional unneeded or rejected copies must be destroyed in accordance with the procedures defined in section 5.7 of this handbook.

If the copier malfunctions and the copy or original cannot be retrieved, the DSO must be notified to ensure that the copier is removed from service until the malfunction has been properly cleared and any copies containing classified information have been extracted from the copier.

5.6.4. Scheduled Maintenance

The DSO must be notified prior to a scheduled service visit for a classified copier, and a cleared individual must be present during the servicing. No maintenance person is permitted to service any equipment used for the reproduction of classified material without a cleared escort. The cleared escort is responsible for:

(a) Collecting any documents, image-retaining drum sheets, or memory chips removed from the machine;

(b) Storing the collected materials in a GSA-approved container until destroyed, if appropriate; and

(c) Ensuring the maintenance person is escorted at all times while servicing equipment used for classified reproduction.

5.7. Destruction of Classified Material

Documents that are no longer required for operational purposes must be disposed of in accordance with the provisions of the Federal Records Act and appropriate implementing directives and records schedules. Material that has been identified for destruction continues to be protected, as appropriate for its classification, until it is actually destroyed.

Classified information identified for destruction must be destroyed completely to preclude recognition or reconstruction of the classified information. Methods and equipment approved for destroying classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition, or pulverizing.

The most common method for CBP offices is destroying through use of cross-cut shredders. Cross-cut shredders currently in use that produce a residue particle size that does not exceed 1/32 inch in width by ½ inch in length may continue to be used for the destruction of classified information until December 31, 2016. Where maintenance is performed on such machines that involves rebuilding the shredder blade assembly, or where new shredders are purchased for the destruction of classified information, the replacement or new purchase must comply with Committee on National Security Systems Policy No. 16, *National Policy for the Destruction of COMSEC Paper Material*, and must be listed on the National Security Administration Evaluated Products List of High Security Crosscut Paper Shredders. A copy of the Evaluated Products List can be obtained from OPR/SMD or the DSO.

Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media can be obtained from OPR/SMD.

5.8. End-of-Day Security Checks

Each CBP office that receives, stores, and/or processes classified information must establish a system of security checks at the close of each working day to ensure that all classified information has been returned to the appropriate GSA-approved security container and is properly secured. Each office is required to visibly display the SF-701 (Activity Security Checklist) to ensure:

(a) All desks and countertops are free of classified information and the information is properly secured;

(b) All communications security (COMSEC) material is secured; and

(c) The SF-702 (Security Container Check Sheet) has been properly completed for the day.

6. Storage

Classified national security information must be afforded a level of protection against unauthorized access and disclosure that is commensurate with its level of classification. Classified information that is not under the personal control and observation of a cleared person is to be guarded or stored in a locked General Services Administration (GSA)-approved security container, vault, room, or area. Any person having access to or possession of classified information is responsible for meeting the accountability and storage requirements prescribed in this handbook.

Classified information must be secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this handbook represent the minimum acceptable security standards.

Sensitive Compartmented Information (SCI) may only be stored in accordance with specifications and requirements of the Office of the Director of National Intelligence. The DHS Special Security Program has oversight in accrediting DHS facilities for the storage of SCI. The Office of Intelligence (OI) is the only CBP office authorized to receive and store SCI within CBP. Any requests for additional facilities for the storage of SCI must be approved by the Assistant Commissioner, OI. OI further coordinates with DHS for Sensitive Compartmented Information Facility accreditations.

For the storage requirements of For Official Use Only information, refer to section 10.8 of this handbook. For storage of Sensitive Security Information, see section 11.10 of this handbook.

6.1. Standards for Storage Equipment

GSA establishes and publishes minimum standards, specifications, and supply schedules for security containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information.

Weapons, sensitive or valuable items (e.g., funds, jewels, precious metals, etc.), seized items (e.g., drugs), or personal papers and effects must not be stored in the same container used to safeguard classified information.

6.1.1. New Purchases

New purchases of combination locks for GSA-approved security containers, vault doors, and secure rooms must conform to Federal Specification FF-L-2740. Existing non-FF-L-2740 mechanical combination locks will not be repaired. If these locks should fail, they must be replaced with locks meeting FF-L-2740 standards. (Note: All newly purchased security containers must be recorded in the Classified Storage Container database maintained by the Office of Professional Responsibility (OPR), Security Management Division (SMD).)

6.1.2. Maintenance

Maintenance performed on GSA-approved security containers must be in accordance with Federal Standard 809A, *Neutralization and Repair of GSA-Approved Containers*. When repairs to a GSA-approved security container affect its original integrity, the GSA-approved label must be removed and the container will no longer be authorized for the

storage of classified information. For security container maintenance or repair issues, contact OPR/SMD or the Designated Security Officer (DSO).

6.2. Top Secret Information

To obtain authorization to store Top Secret information or material within their facility, CBP offices must submit a written request to OPR/SMD for review and approval. Approval or denial of the request is based on a review of physical security measures and proposed supplemental controls.

Top Secret information must be stored in a GSA-approved security container or a modular vault or a secure room constructed in accordance with Federal Standard 832, *Construction Methods and Materials for Vaults*, and equipped with an intrusion detection system (IDS), with cleared personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth, or within 5 minutes of the alarm if it is not.

When Top Secret information is stored in a GSA-approved security container, one of the following supplemental controls must be in place:

(a) Guard or duty personnel possessing a minimum of a final adjudicated Secret clearance inspect the security container once every two hours;

(b) An IDS is in place with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; or

(c) Security-In-Depth coverage of the area in which the container is located, provided the container is equipped with a lock meeting Federal Specification FF-L-2740.

Security-in-depth means a determination by the agency head that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an IDS, random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

6.3. Secret Information

Secret information must be stored by one of the following methods:

(a) In the same manner as prescribed for Top Secret information; or

(b) In a GSA-approved security container or vault without supplemental controls.

6.4. Confidential Information

Confidential information must be stored in the same manner as prescribed for Top Secret or Secret information, except that the supplemental controls are not required.

6.5. Open Storage

Approval of open storage is considered when the volume of material or operational necessity of the mission dictates. OPR/SMD is responsible for issuing approvals. Refer

to DHS Instruction 121-01-011, Chapter 4 (Safeguarding and Storage), for additional information.

6.6. Identification of Security Containers

There must be no external mark revealing the level of classified information authorized for, or actually stored in, a given security container, nor indicating the priority assigned to the container for emergency evacuation and destruction.

Each security container must be marked for accountability and ready identification. This can be accomplished in a variety of ways, including use of the existing property control number. An internal or local system must be established by which each security container in use (other than vaults/secure areas) can be easily identified by a consecutive number, without regard to physical location of the container. The identification numbers must be affixed to each container where they will be conspicuously visible.

For control and tracking purposes, all security containers must be entered into OPR/SMD's Classified Storage Container database.

6.7. Protection of Classified Combinations

Combinations to security containers, vaults, or other areas approved for the storage of classified national security information must be recorded on the SF-700 (Security Container Information). The SF-700 must be completed accurately and reflect all pertinent information, such as the container's location, description/type, names of personnel with access to the combination, etc.

Knowledge of combinations must be limited to the minimum number of persons necessary for operating purposes. The combination of a container, vault, or secure room used for the storage of classified information is afforded the same protections as the highest level of classified information stored therein. Any written record of a classified combination is marked with the appropriate classification level. Combinations must not be stored in calendars, rolodexes, desk drawers, key-locked cabinets, wallets, electronic files, at home, etc. The storage or recording of combinations to security containers anywhere other than on the required SF-700 is considered a security violation.

An SF-700 must be completed for each lock (including containers that have multiple locks) and marked with the highest classification level that the security container is approved to store. Upon completion of Part 2A, the SF-700 becomes a classified document and must be treated as such. When completed, the SF-700 must be separated into three parts:

(a) Part 1 must be affixed to the inside of the security container (close to the lock) and be visible when the container is open.

(b) Part 2A, containing the written combination, must be sealed inside Part 2.

(c) Part 2 must be stored in a separate security container as follows:

   i. CBP headquarters and facilities located within the National Capital Region must forward the SF-700, Part 2, to OPR/SMD for storage.

ii. CBP field offices must forward the SF-700, Part 2, to the director of the appropriate Field Office, Sector Headquarters, or regional office for storage.

An SF-700 containing the combination of a container, vault, or secure room used for storage of classified information or material must be afforded protection equal to that given to the highest level of classified information stored in the container.

6.8. Access to Classified Combinations

Only appropriately cleared and authorized personnel may have access to classified combinations. The number of individuals with access must be kept to a minimum. Contact information must be annotated on the SF-700, in case the container is ever found open and unattended.

6.9. Changing Combinations

Combinations to security containers may be changed by OPR/SMD or by other authorized personnel, such as the designated Classified Document Custodian (CDC). Combinations must be changed under the following conditions:

(a) When first placed in use;

(b) When an individual who knows the combination no longer requires access to it, unless other sufficient controls exist to prevent access to the lock;

(c) When the combination has been subjected to actual or possible compromise;

(d) Every two years, if none of the above has occurred; or

(e) When taken out of service. (Built-in combination locks must be reset to the standard combination 50-25-50 and combination padlocks must be reset to the standard combination 10-20-30.)

6.10. Security Container Check Sheet

An SF-702 (Security Container Check Sheet) must be placed on the exterior of each security container to record every time the container is opened, closed, and checked. Each opening and closing of the container must be recorded using the initials of the individual conducting the action and the time of the opening or closing. The “Checked By” column must 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-day security 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 in the same direction. Although it may not always be possible, the person conducting the end-of-day security check of the container 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 classified information in the office is protected. Supervisors are responsible for establishing procedures to ensure that these requirements are met.

6.11. Annual Security Container Inventory

Within CBP, each program office that handles and stores classified information is required to conduct an annual inventory of classified material stored within the office's security container(s). The annual security container inventory must be conducted by September 30 of every year (once each fiscal year). The DSO is responsible for ensuring that the designated CDC perform the annual inventory on all security containers for which the CDC is responsible. The CDC must report the results of the inventory, including any noncompliant findings, to the DSO. The DSO will report completion of the inventory to OPR/SMD as part of the annual reporting requirements.

The purpose of the annual security container inventory is to identify and properly destroy any classified materials that are no longer required for the office's current or future program activities or operations. Annual inventories are also conducted to ensure that only materials classified at or below the highest level of classification authorized for storage are contained in the security container.

Any incident in which classified information is not stored by an approved means, such as Top Secret information stored in a security container authorized for storage of classified material up to the Secret level, is considered a security incident and must be reported in accordance with section 8.1 of this handbook.

6.12. Security Container Turnover Process

Under certain circumstances, CBP program offices that handle and store classified information are required to conduct a security container turnover process in the event that a senior CBP official who previously had access to a security container no longer requires such access.

When a senior CBP official (i.e., an employee serving in a GS-15 level position or Senior Executive Service position) resigns, transfers, or otherwise departs from a CBP position in which he or she had access to a classified security container, the CBP program office with responsibility for the container must conduct an inventory and turnover of its contents. A CBP employee who is authorized to access the classified security container (e.g., one of the individuals listed on the security container's SF-700 and/or the designated CDC) must carry out the review and turnover process. See Appendix E for required security container turnover procedures.

The purpose of the security container turnover process is to identify and properly destroy any classified materials that are no longer required for a CBP office's programs and operations, following the departure of a senior CBP official. The process is also required to ensure that only materials classified at or below the highest level of classification authorized for storage are contained in the security container to which the senior CBP official had access.

6.13. Residential Storage

The DHS Chief Security Officer may authorize the storage of classified information in private residences. Requests for in-residence storage of classified information are submitted with justification through OPR/SMD to the DHS Chief Security Officer.

When residential storage is approved, a GSA-approved security container or other container approved by the DHS Office of the Chief Security Officer (OCSO),

Administrative Security Division (ASD) is furnished. For storage of Top Secret information, an intrusion detection alarm system meeting Underwriters Laboratories (UL) standards is also in place and operational. Written procedures are developed to provide for the appropriate protection of the information, to include a record of the information that is authorized for residential storage. These procedures are coordinated through DHS OCSO/ASD.

6.14. Security Containers Taken Out of Service

Security containers no longer used for the storage of classified information may be transferred to other areas where they are needed or stored as surplus. Prior to removing any container, the container must be thoroughly searched to ensure all classified information has been removed. Areas to be searched include behind, beneath, and on the sides of the container and behind, under, and on the sides of all drawers. The person who conducts the search must declare the container empty by placing a written statement on the outside front of the container indicating the date of the inspection, the name of the person who conducted the inspection, and the office that last used the container. In addition, prior to removing any security container with a built-in combination dial, the combination must be reset to the standard combination of 50-25-50. The written statement on the outside of the container must identify that the combination has been reset. The security contact must remove and destroy Part 1 of the SF-700 located inside the control drawer.

Security containers may not be relocated or taken out of service without first notifying OPR/SMD and/or the appropriate DSO. Prior to transferring or excessing a security container, the information must be properly documented in OPR/SMD's Classified Storage Container database for control and tracking purposes.

6.15. Storage in Foreign Countries

Except for classified information that has been authorized for release to a foreign government, U.S. classified information may be retained in foreign countries only when necessary to satisfy specific U.S. government requirements. Classified material in foreign countries must be stored in one of the following locations:

(a) A U.S. military installation, or a location where the United States holds extraterritorial status, such as an embassy or consulate;

(b) A U.S. government entity located in a building used exclusively by U.S. government tenants provided the building is under 24-hour control by U.S. government personnel;

(c) A U.S. government entity located in a building not used exclusively by U.S. government tenants, or under host government control, provided the classified material is stored in GSA-approved security containers and under 24-hour control by U.S. government personnel; or

(d) A U.S. government entity located in a building not used exclusively by U.S. government tenants, but that is under host government control, provided the classified material is stored in GSA-approved security containers that are further secured in a locked room or area to which only U.S. government personnel have access.

6.16. Computer Equipment and Removable Storage Media

Classified information must not be processed on any equipment unless it has been certified and accredited for classified processing (see the CBP National Security Systems Handbook, HB 1400-06). CBP security procedures prescribe the appropriate safeguards to:

(a) Prevent unauthorized access to the equipment and/or information;

(b) Replace and destroy equipment parts as classified material when the information cannot be removed from the parts or protected appropriately, commensurate with the level of classification; and

(c) Ensure that appropriately cleared and technically knowledgeable personnel inspect equipment before the equipment is removed from protected areas.

7. Transmission and Transportation

Classified information must be transmitted and received pursuant to the standards cited in this handbook and in a manner that ensures tampering can be detected, inadvertent access is precluded, and timely delivery to the intended recipient is assured. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized to receive the information, are aware of the transmission, and have the capability to safeguard it properly. Under no circumstances may classified information be transmitted by any means other than the approved methods described in this handbook.

7.1. Methods of Transmission and Transportation

7.1.1. Transmission of Top Secret

Top Secret information must be transmitted by:

(a) Direct contact between appropriately cleared persons;

(b) Secure terminal equipment or secure fax keyed to the Top Secret level;

(c) Defense Courier Service or other authorized government agency courier service;

(d) Department of State courier system (also known as a diplomatic pouch); or

(e) Electronic means over cryptographic communications systems approved by the National Security Administration.

Under no circumstances may Top Secret information be transmitted via the U.S. Postal Service or any other uncleared commercial delivery service.

7.1.2. Transmission of Secret and Confidential

Secret and Confidential information must be transmitted by:

(a) Any of the methods approved for transmitting Top Secret information;

(b) U.S. Postal Service Registered Mail;

(c) U.S. Postal Service Express Mail. When using U.S. Postal Service Express Mail, the Waiver of Signature and Indemnity block (Item 11-B) on the U.S. Postal Service Express Mail label is not executed. Additionally, street-side collection boxes must not be used; or

(d) Commercial carriers or commercial messenger services cleared for such purposes under the National Industrial Security Program.

7.1.3. Transmission of Classified Information outside the United States

Transmitting classified information to a Federal government facility located outside of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Commonwealth of the Northern Mariana Islands, Guam, and any other territory or possession of the United States, must be by methods commensurate with the level of classified information being transmitted. U.S. Registered Mail through Military Postal Service facilities may be used to transmit Secret and Confidential information provided

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.

7.1.4. Transmission of Classified Information to Foreign Governments

Transmission of classified information to foreign governments must be approved in accordance with DHS foreign disclosure policies and procedures.

7.2. Shipment of Freight

Transmitting bulk classified material must be performed by qualified, cleared carriers that are authorized to transport material via a Protective Security Service under the Department of Defense Industrial Security Program. This may be done only within the United States when the size, bulk weight, and nature of the shipment make other methods impractical.

Observation is not required while the shipment is stored in an aircraft or ship in connection with air or sea transport provided the shipment is in a compartment that is not accessible to unauthorized persons or is loaded in specialized shipping containers, including closed cargo containers. The container or compartment must be sealed to prevent access without detection.

Cleared operators, officers of ships, or pilots of aircraft who are U.S. citizens may be designated as escorts, if control and surveillance of the cargo is maintained 24 hours a day. The escort must protect the shipment at all times through personal observation, placing the shipment in protected storage or other measures designed to prevent inspection, tampering, pilferage, or other unauthorized access.

All additional control notices imposed by an original classification authority must be honored when transmitting and transporting classified national security information.

7.3. Preparation of Material for Transmission

All classified information physically transmitted outside CBP facilities must be enclosed in two layers, both of which conceal the contents, prevent inadvertent opening, and provide reasonable evidence of tampering. When envelopes are used, they must be sealed with reinforced tape.

The inner enclosure must clearly identify the name of the intended recipient, the address of both the sender and the recipient, the highest classification level of the contents, and any appropriate warning notices.

The outer enclosure must clearly identify the office of the recipient (personal names must not be used) and the addresses of both the sender and the recipient. There are no markings on the outside envelope to indicate that the contents are classified. Intended recipients are identified by name only on the inner envelope. The following exceptions apply:

(a) If the classified material is an internal component of a packable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information.

(b) If the classified material is an item of equipment that is not reasonably packable and the shell or body is classified, it must be concealed within an opaque enclosure that hides all classified features.

(c) Specialized shipping containers, including closed cargo transporters or diplomatic pouches, may be considered the outer enclosure when used.

(d) When classified information is hand-carried outside a facility, a locked briefcase or similar locking container may serve as the outer enclosure.

The Office of Professional Responsibility (OPR), Security Management Division (SMD) may approve the use of specialized shipping containers that are secured with a high-security padlock and equipped with an electronic seal that would provide evidence of surreptitious entry. Such containers must be sufficiently constructed to provide evidence of forced entry and are handled by the carrier to ensure that the container is protected until its delivery is completed.

7.4. Escorting or Hand-Carrying of Classified Material

7.4.1. Courier Authorization

Courier authorization is issued to individuals who hand-carry classified information outside and beyond the perimeter of a building or compound. Courier authorization requests are processed and approved by OPR/SMD. Requests for courier authorization must be submitted to OPR/SMD using DHS Form 11000-2 (Courier Authorization Request). The individual's security clearance level must be equal to or higher than the level of material being carried. Courier requests are only granted up to the level of the material to be transported, which may not be equivalent to the individual's clearance level. Designated couriers are required to review the *Guidance for Classified Couriers* briefing pamphlet and must sign a form acknowledging receipt of the card and understanding of the information contained in the briefing pamphlet.

(a) OPR/SMD will issue a one-time courier letter instead of a courier card when the designated courier is required to hand-carry classified information on an infrequent basis within the local commuting area. Such letters have an expiration date not to exceed 30 days from the date of issuance.

(b) OPR/SMD will issue a permanent courier card when the designated courier is required to frequently and routinely hand-carry classified information within the local commuting area. Such cards have an expiration date not to exceed two years from the date of issuance. DHS Form 11000-1 (Classified National Security Information Courier Card) is used for this purpose.

7.4.2. Courier Travel by Commercial Air

Transporting classified material aboard commercial aircraft is strongly discouraged and requires prior approval by OPR/SMD. Commercial air transportation is approved only in instances of great urgency or when the material cannot be transmitted by other means.

The request for transport aboard commercial aircraft, with justification, must be submitted to OPR/SMD using DHS Form 11000-2. The justification section must clearly indicate that the courier will be transporting classified information via commercial air.

OPR/SMD will approve or disapprove the request based on the justification provided. If approved, a courier authorization letter will be issued by OPR/SMD.

Couriers who are authorized to travel by commercial aircraft are required to transport classified materials in their carry-on luggage. Refer to the *Guidance for Classified Couriers* briefing pamphlet for additional information.

If information technology equipment (e.g., laptop computer, computer media, etc.) containing classified information is to be transported, it must be encrypted prior to transport. Refer to the CBP Information Systems Security Policies and Procedures Handbook, HB 1400-05D, for additional information.

7.4.3. Transportation of Classified Material within an Activity or Office

Courier authorization is required to transport classified material from one building to another via a public street or road. The material must be packaged in accordance with the requirements defined in this handbook.

If required to transport classified material within the same building or compound, an appropriate cover sheet (SF-703, *Top Secret*; SF-704, *Secret*; or SF-705, *Confidential*) must be affixed to the document, and the document must be placed in an unmarked envelope or folder to avoid inadvertent disclosure. Courier authorization is not required.

7.5. Receipts

Receipts for Top Secret and Secret materials transmitted or transferred outside of CBP must be returned to the transmitting office within 30 days. DHS Form 11000-11 (Record of Transmittal for Classified Documents or Other Accountable Material) is used for this purpose. See section 5.5 of this handbook for additional guidance on maintaining receipts for the transmission of classified material outside of CBP.

8. Security Incidents

Programs and safeguards established for the identification and protection of classified information are necessary to ensure U.S. national security. Incidents involving the mishandling of classified information are promptly and thoroughly investigated to determine the cause, assess and mitigate potential damage, and implement measures to prevent recurrence.

For information about security incidents involving the improper handling of For Official Use Only information, refer to section 10.10 of this handbook. For security incidents involving Sensitive Security Information, see section 11.14 of this handbook.

8.1. Reportable Security Incidents

Security incidents must be reported promptly, but no later than 24 hours after the time of discovery. DHS Form 11000-10 (Report of Security Incident) is used for this purpose. All security incidents involving the mishandling of collateral classified information must be reported to the Office of Professional Responsibility (OPR), Joint Intake Center as follows:

Phone: 1-877-2INTAKE (1-877-246-8253)
Email: Joint.Intake@dhs.gov

Reportable security incidents include, but are not limited to:

(a) Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(b) Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 13526 and its implementing directives;

(c) Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of E.O. 13526 and its implementing directives;

(d) Any incident involving computers or telecommunications equipment or media that may result in disclosure of classified information to unauthorized individuals; or any incident that results in the unauthorized modification or destruction of classified system data, the loss of classified computer system processing capability, or the loss or theft of classified computer system media;

(e) Any incident involving the processing of classified information on computer equipment that has not been specifically approved and accredited for that purpose by an authorized official;

(f) Any incident involving the transmission or transportation of classified information by an unapproved method, or any evidence of tampering with a shipment, delivery, or mailing of packages containing classified information;

(g) Any incident in which classified information is not stored by an approved means;

(h) Any incident in which classified information is inadvertently revealed to or released to a person who is not authorized access;

(i) Any incident in which classified information is destroyed by unauthorized means;

(j) Any incident in which classified information is reproduced without authorization or contrary to specific restrictions imposed by the originator or on equipment that has not been specifically approved and accredited for that purpose; or

(k) Any other incident in which classified information is not safeguarded or handled in accordance with prescribed procedures.

8.2. Incidents Involving Sensitive Compartmented Information

Incidents involving Sensitive Compartmented Information (SCI), Special Access Program information, and all other incidents that occur within a Sensitive Compartmented Information Facility must be reported to the Office of Intelligence (OI) Special Security Officer.

8.3. Preliminary Inquiry

Upon notification of an alleged security incident, the OPR Security Management Division (SMD) will initiate a preliminary inquiry. In cases involving SCI, OI will initiate the inquiry. The person conducting the preliminary inquiry serves as the Inquiry Official. The Inquiry Official has the authority to conduct interviews and obtain statements from personnel knowledgeable about the incident. Personnel involved in the inquiry process are required to cooperate with Inquiry Officials. Failure to cooperate can result in sanctions, as described in section 8.8 of this handbook.

The preliminary inquiry and corresponding Memorandum for Record (MFR) must be completed within 15 work days from the date of initiation. Where a preliminary inquiry cannot be completed within 15 work days, the Inquiry Official will include a statement in the MFR justifying the delay.

A preliminary inquiry is conducted to determine:

(a) Whether a security violation or infraction occurred;

(b) Time, date, and location of the alleged incident;

(c) Whether there was an actual compromise or a suspected compromise of classified information;

(d) Identification of the classified information involved;

(e) The person(s) responsible for and involved in the security violation or infraction;

(f) The cause of the security violation or infraction;

(g) The actions taken to minimize damage or neutralize the potential for compromise; and

(h) Recommendations to prevent recurrence of similar security incidents, to include additional training or procedural changes.

If the security incident involves the improper transmission of classified information to CBP from an outside agency, the Inquiry Official will notify the security official of the sending office or agency, who will pursue the matter further in accordance with the sending agency's regulations. For incidents involving classified spillage, the CBP

Computer Security Incident Response Center (CSIRC) will conduct damage control of the affected CBP automated systems to remove any trace of the classified information.

If the security incident involves the improper transmission of classified information to CBP from another DHS component, the Inquiry Official will notify the appropriate security official of the sending component for resolution of the matter by the sending component pursuant to its regulations.

8.3.1. Damage Assessments

If the preliminary inquiry reveals an actual compromise or a suspected compromise to classified information, the Inquiry Official will request that the original classification authority (OCA) with jurisdiction over the information conduct a damage assessment.

(a) If classified information originated by a CBP OCA is compromised, the MFR and request for damage assessment will be forwarded to the Assistant Commissioner, OPR, for processing.

(b) If another government agency's classified information is compromised, a copy of the MFR and request for damage assessment will be forwarded to the applicable government agency.

(c) If the originator of information involved in a security incident cannot be determined, the MFR will be forwarded to the DHS Office of the Chief Security Officer (OCSO), Administrative Security Division (ASD). DHS OCSO/ASD will attempt to determine the originator of the information and process the damage assessment request. If the originator cannot be determined, DHS OCSO/ASD will seek guidance from the Information Security Oversight Office.

8.3.2. Inadvertent Disclosure Statement

If the incident involves the inadvertent disclosure of classified information to a person not authorized access, the person who received the information will be asked to sign an Inadvertent Disclosure Statement (see Appendix F for a copy of the Inadvertent Disclosure Statement form). If the individual refuses to sign the Inadvertent Disclosure Statement, the information on the form must be read orally to the person in the presence of a witness, and the form is annotated to reflect the individual's refusal to sign. Both the Inquiry Official and the witness must sign the form. This information will be included in the MFR.

8.3.3. Memorandum for Record

If the MFR contains classified information, it must be handled and marked accordingly. At a minimum, the MFR must be marked and handled as "For Official Use Only."

Persons who are suspected or found to have committed a security violation or infraction will be afforded the opportunity to provide a written statement disputing the facts or identifying mitigating circumstances. Such written statements will be included as an attachment to the MFR.

A copy of the MFR will be retained by OPR/SMD. Where a person is found to have committed a security violation, a copy of the MFR and all other supporting documentation will also be included in the individual's personnel security file. Upon

receipt, the OPR Personnel Security Division reviews the MFR to determine if suspension or revocation of a security clearance is appropriate.

MFRs pertaining to incidents involving contract employees will be provided to the applicable Contracting Officer's Representative or equivalent Federal employee having oversight of the contract. In addition, further reporting relative to contractors will be made in accordance with the National Industrial Security Program Operating Manual.

An MFR will be sufficient to close the incident if it is determined that:

(a) The loss or compromise of classified information has not occurred or its likelihood is remote.

(b) The compromise of classified information has occurred, but there is no indication of knowing, willful, or negligent behavior or significant security weaknesses.

(c) There is no evidence of employee misconduct, criminal behavior, or espionage.

(d) No additional information is likely to be obtained by conducting a formal investigation.

8.4. Formal Investigation

The decision to conduct a formal investigation in lieu of or subsequent to a preliminary inquiry is made by the OPR Investigative Operations Division (IOD).

Upon determination that a formal investigation is appropriate, OPR/IOD will conduct the investigation accordingly. Should the DHS Office of Inspector General, the Federal Bureau of Investigation, or another agency assume investigative responsibility, CBP will coordinate all further actions with that investigative agency.

Reports of investigations are forwarded to the OPR Joint Intake Center.

8.5. Classified Spillage

Classified spillage is the accidental, inadvertent, or intentional introduction of classified information into information technology (IT) systems not specifically certified and accredited for classified use, or certified and accredited at a level lower than that of the classified information introduced into it. Classified spillages can pose a significant threat to the confidentiality, integrity, and availability of CBP IT systems. Immediate action must be taken to assess and mitigate the incident. Assessment includes an immediate determination as to whether or not a spillage occurred.

Classified spillages must be reported immediately to a supervisor and the CBP CSIRC by secure means in accordance with the CBP Information Systems Security Policies and Procedures Handbook, HB 1400-05D.

Users must take no action to delete, disturb, or further disclose spilled information, such as deleting an email that contains classified information or a classified attachment, or printing hard copies of the information on an unclassified printer.

Specific information regarding a spillage is classified at the same level of the information spilled until confirmation is received that the spilled information has been effectively eradicated from the IT system or that the potential for compromise has been otherwise

neutralized. Specific information means information sufficient to allow a dedicated intruder or curiosity seeker to search for and access the spilled material.

The CBP CSIRC is responsible for forwarding incident reports to the OPR Joint Intake Center for preliminary inquiry or formal investigation.

8.6. Overseas Security Violations and Infractions

Security incidents occurring at overseas locations are under the purview of the Department of State (DOS). If a security incident involving CBP personnel occurs at an overseas location, the DOS Regional Security Officer, U.S. Marine Corps Security Guard, or other designated officials must be notified directly.

DOS will notify DHS OCSO of security incidents occurring at overseas locations involving CBP personnel via an Optional Form (OF) 117 (Notice of Security Violation). DHS OCSO will forward this form to OPR/SMD to initiate a preliminary inquiry.

8.7. Other Agency Security Violations and Infractions

CBP personnel who observe or learn of a security incident caused by a visiting or detailed employee or contractor of another agency must report the incident in accordance with the guidelines provided in section 8.1 of this handbook.

The Assistant Commissioner, OPR, will send a memorandum to the security office of the visiting or detailed individual's agency with a description of the incident.

8.8. Sanctions

When an individual is found to be responsible for the commission of a security violation or infraction, the employee may be subject to administrative, disciplinary, or criminal sanctions. The type of sanctions imposed is under the purview and authority of appropriate supervisory/management officials and is based on several considerations, including the following:

(a) The severity of the incident;

(b) The intent of the person committing the security violation or infraction;

(c) The extent of information security training the person has received; and

(d) The frequency of which the individual has been found responsible for prior security violations or infractions.

Sanctions include, but are not limited to, verbal or written counseling, reprimand, suspension from duty and pay, removal, suspension or revocation of access to classified information, termination of classification authority, or criminal penalties.

Administrative sanctions are assessed in accordance with the policies, procedures, and practices established by the Office of Human Resources Management, Labor and Employee Relations office, and actions involving the suspension or revocation of a security clearance are taken in accordance with the applicable executive orders and Office of the Director of National Intelligence policies and regulations.

Where a proposed sanction associated with the unauthorized disclosure of classified information is in excess of a reprimand, the official imposing the sanction will first coordinate with the CBP Office of the Chief Counsel (OCC) for legal review prior to imposing the sanction. Further, where a criminal violation has occurred that may result in a criminal prosecution, the investigating agency will coordinate with OCC, which will coordinate with the Department of Justice as appropriate.

9. Industrial Security Program

This chapter sets forth the policies and procedures for CBP's participation in the National Industrial Security Program (NISP). Established by E.O. 12829 on January 6, 1993, the NISP provides for the protection of classified information as defined by E.O. 13526 and the Atomic Energy Act of 1954.

The NISP serves as a single integrated and cohesive program for the protection of classified information when not in Federal government possession. Under the NISP, contractors are mandated to protect all classified information to which they have been given access or custody by the Federal Government.

DHS entered into a Memorandum of Agreement with the Department of Defense (DOD) on August 22, 2003. The agreement authorizes DOD to act for and on behalf of DHS in rendering security services for the protection of classified information released by DHS to or within industry. DHS participates in the NISP to ensure that any classified information released to or accessed by industry, in connection with DHS contracts, grants, or related activities, is properly safeguarded in accordance with E.O. 13526.

Participation in the NISP allows DHS to use the Defense Security Service (DSS) to conduct investigations of contractor facilities and personnel security clearances, and to monitor the contractors' compliance with safeguarding requirements. All facility and personnel security clearances granted by DOD are accepted by DHS as establishing eligibility for access to classified information. Upon completion by DSS of all investigative requirements, facilities are considered eligible for access to classified information, or contract award, at the appropriate level granted by DSS.

DSS issues and maintains facility security clearances and personnel security clearances, as required, for DHS contractors. DSS inspects and monitors contractors that require or will require access to classified information. The Defense Industrial Security Clearance Office (DISCO), a field element of DSS, issues personnel security clearances for contractors under the authority of the NISP.

9.1. Personnel Security Clearances

To ensure that classified information entrusted to private industry is properly safeguarded, CBP requires that contractors who will require access to classified information in the completion of their contractual responsibilities be processed for security clearances in accordance with the requirements stipulated in the National Industrial Security Program Operating Manual (NISPOM).

Individuals employed by a contractor will be cleared through DSS/DISCO. The cleared contractor is required to have a designated facility security officer (FSO) through whom requests for personnel security clearances are submitted to DISCO. The FSO must provide the Contracting Officer's Representative with an updated status report of security clearance actions required, pending, and approved. The FSO is also responsible for submitting visitor authorization requests for cleared employees intending to visit CBP facilities. Contractor personnel must have security clearances commensurate with the level of access required for performance under the contract. CBP has no role in the processing or granting of security clearances to industry personnel.

For consultants who are working on an interagency agreement, the consultant's agency will provide the security clearance. The consultant and the Office of Professional Responsibility (OPR), Security Management Division (SMD) will execute a security agreement, which will identify the consultant's responsibilities and any accesses required. A DD Form 254 (Contract Security Classification Specification) is not needed. If the individual will require access to Sensitive Compartmented Information (SCI) and does not currently have access, the individual must send justification to the FSO in the form of a nomination letter. The FSO must package the documentation, submit it to the CBP Special Security Officer in the Office of Intelligence for processing, and provide a copy of the security agreement to the DHS Office of the Chief Security Officer (OCSO).

For independent consultants, the Office of Human Resources Management notifies OPR/SMD that a consultant will be brought on board and then sends a copy of the consultant agreement to OPR/SMD. OPR/SMD completes the security agreement and sends it and the nondisclosure agreement to the hiring office for signature. The signed security agreement and nondisclosure agreement are kept on file.

9.2. Facility Security Clearances

Any firm or business under contract with CBP that requires access to classified information must possess a facility security clearance commensurate with the level of access required. This includes any firm or business entity that requires access to classified information to prepare a response to a request for proposal (RFP) or a request for bid and/or in performance of a classified contract.

Firms that do not possess a facility security clearance, or the requisite level of facility security clearance, must be sponsored for a DOD facility security clearance when a determination has been made by the CBP program office that the contract effort will require access to classified information. CBP offices must submit relevant sponsorship requests for facility security clearances to OPR/SMD for processing through DSS.

Facility security clearances for subcontracts must be sponsored and processed by the prime contract in accordance with the NISPOM.

DSS will conduct a risk assessment for all contracts that require contractors to store, process, or access classified CBP information, systems, or property at a contractor facility to identify countermeasures and ensure such countermeasures are implemented prior to the contractor gaining control of CBP material.

The cognizant DSS office will provide physical security oversight for cleared contractor facilities.

DHS OCSO will provide oversight of SCI and Special Access Programs (SAPs).

9.3. Contract Security Classification Specification (DD Form 254)

In order to activate DSS services and obligate the contractor to adhere to the provisions of the NISPOM, CBP offices must include a DD Form 254 in all classified contracts and classified contract solicitations. The DD Form 254 is the primary vehicle for relaying contract-specific security classification guidance to the contractor and therefore, in section 13 of the form, identifies the sources from which the contractor derives security classification requirements. The sources either identify any published security classification guides applicable to the contract effort, or base classification on existing

classified information from which the contractor must derive and apply classification guidance. Where a source is identified as a security classification guide, the contractor must be provided access to, or a copy of, the applicable guide.

A DD Form 254 is completed only for contracts that require access to classified information.

CBP offices must provide the statement of work or other documentation that describes the services or supplies to be provided by the contractor to OPR/SMD for assistance in verifying classification requirements and preparing the DD Form 254.

The contract, statement of work, or other documentation must contain Federal Acquisition Regulation (FAR) Security Clause 52.204-2, stating that a government contracting officer made a determination that the contract issued will require access to classified information by the contractor or the contractor's employees in the performance of the contract. In addition, Homeland Security Acquisition Regulation Clause 3052.204-71 mandates that contractors requiring unescorted access to government facilities, access to sensitive information, or access to government information technology resources are required to have a favorably adjudicated background investigation prior to commencing work on the contract. This requirement is prescribed for all CBP classified contracts and is applicable to all phases of pre-contract activity, including solicitations (bids, quotes, and proposals), pre-contract negotiations, post-contract activity, or other government contracting activity programs that require access to classified information by a contractor. In addition, such documentation must also identify the classification level (Top Secret, Secret, or Confidential).

OPR/SMD will return the approved DD Form 254 to the Contracting Officer's Representative for inclusion in the contract or solicitation. OPR/SMD will distribute a copy of the DD Form 254 to DSS and DHS OCSO. DSS will conduct investigations and issue personnel security clearances for the contract employees. DSS will also provide security oversight functions in coordination with the contractor's FSO, with the exception of "carve out" contracts requiring access to SCI or SAPs. The DHS OCSO Special Security Programs Division will provide oversight for contracts involving access to SCI and SAP information.

In some instances, it may be necessary to include classified information in a DD Form 254. In those cases, the documentation must be protected in a manner approved for classified information.

9.4. Processing Requirements

For each classified contract, the contract solicitation must include a statement that the contractor will require access to classified information and/or will generate classified information in the performance of the contract.

OPR/SMD must verify all facility security clearances for classified contracts.

The contract, statement of work, or other documents will contain a security clause stating that a government contracting officer made a determination that the contract will require access to classified information by the contractor in the performance of the contract.

The DD Form 254 is reviewed to ensure that all of the security requirements captured in the statement of work are also identified in the DD Form 254.

9.5. Classified Visits

OPR/SMD will accept visit authorization letters only when the letters are submitted in accordance with Chapter 6 of the NISPOM.

All classified visits by contractors require advance notification to the office hosting the visit. Requests must be in writing and may be submitted by mail, fax, or email. Hand-carried visit requests will not be accepted. OPR/SMD has final approval authority for the proposed visit. If OPR/SMD disapproves a visit, the requester will be promptly notified.

Visitors are not to take notes, make records of classified discussions, discuss classified information on non-secure telephones, or take photographs in areas where classified information might be recorded, unless given permission by the hosting program office.

CBP offices must ensure that visitors are not granted access to classified information higher than the level of each visitor's security clearance, as certified in the visit authorization letter.

Classified visit requests are coordinated through the OPR Personnel Security Division for clearance verification.

9.5.1. International Security Agreements

International Security Agreements with foreign governments address security controls, protection, and assurance for safeguarding classified information. These agreements establish the "government-to-government" principle, signifying that signatory governments each have legal responsibility over the others' classified information at all times. All agreements must be in accordance with Chapter 10 of the NISPOM.

DHS OCSO is responsible for the administration and oversight of classified material to be exported (i.e., any disclosure or transfer of technical data to a foreign national), the permanent and temporary import of classified information, and compliance by cleared U.S. contractors involved with the North Atlantic Treaty Organization (NATO), foreign governments, and foreign contractors.

DHS OCSO maintains a record of cleared U.S. contractors involved with foreign entities and related activities. Any offices and contractors desiring to enter into international agreements must report their intentions to DHS OCSO. The report must contain:

(a) The name of the country;

(b) The name and address of the government entity issuing the contract;

(c) The contract or RFP number;

(d) The name of the U.S. contractor and any subcontractors involved; and

(e) The contract/RFP issue and response dates.

Contractors are still required to report their activities to DSS per the NISPOM. DHS OCSO uses this report to issue proper guidance to CBP and contractors to ensure

compliance with governing export control laws (e.g., the Export Administration Regulation and the Arms Export Control Act) before executing any agreement with a foreign interest that involves access to DHS classified information by a foreign national. Contractors are still required to comply with foreign ownership, control, or influence requirements per the NISPOM. Prior to the execution of such agreements, review and approval are required by the Department of State, and release of the classified information must be approved by DHS. Failure to comply with Federal licensing requirements may render a contractor ineligible for a facility security clearance.

9.6. Contract Reviews

OPR/SMD conducts biennial audits of CBP contracts to ensure compliance with applicable DHS security requirements, FAR security clauses, and E.O. 12829. During the contract review process, OPR/SMD identifies classified contracts that do not contain the required DD Form 254, which ensures the required agreements and protections are in place as defined in the NISPOM. Corrective action must be taken to address any noncompliant contracts identified during the audit process.

10. Sensitive But Unclassified (For Official Use Only) Information

For Official Use Only (FOUO) is the designator used within DHS to identify unclassified information that is not otherwise governed by statute or regulation, and 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.

Other government agencies and international organizations use different terminology to identify sensitive information, such as "Limited Official Use (LOU)" and "Official Use Only (OUO)." In most instances, this information is equivalent to FOUO information and must be protected as such. Individuals must ensure all security requirements beyond those identified in this handbook are applied when handling other agency information.

10.1. Categories of FOUO

The types of information listed below are treated as FOUO information. Where information also meets the standards for designation pursuant to other existing statutes or regulations, the applicable statutory or regulatory guidance will take precedence. For example, should information meet the standards for designation as Sensitive Security Information (SSI), then SSI guidance for marking, handling, and safeguarding takes precedence.

(a) Information of the type that may be exempt from disclosure per 5 U.S.C. § 552 (Freedom of Information Act) and its amendments. Designation of information as FOUO does not imply that the information is already exempt from disclosure under the Freedom of Information Act (FOIA). Requests under the FOIA, for information designated as FOUO, will be reviewed and processed in the same manner as any other FOIA request;

(b) Information exempt from disclosure per 5 U.S.C. § 552a (Privacy Act of 1974);

(c) Information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements;

(d) Other international and domestic information protected by statute, treaty, regulation or other agreements;

(e) Information that could be sold for profit;

(f) Information that could result in physical risk to personnel;

(g) DHS information technology internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under E.O. 13526 will be classified as appropriate;

(h) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation;

(i) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under E.O. 13526;

(j) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security; and

(k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

10.2. Designation Authority

Any DHS employee, detailee, or contractor can designate information as FOUO provided it meets the sensitivity threshold defined in DHS Management Directive (MD) 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, and falls within one of the categories of FOUO listed in the MD. Officials occupying supervisory or managerial positions are authorized to designate other information not listed in DHS MD 11042.1 and originating under their jurisdiction as FOUO.

10.3. Duration of Designation

Information designated as FOUO will retain its designation until determined otherwise by the originator or a supervisory or management official having program management responsibility over the originator and/or the information.

10.4. Marking

Information designated as FOUO must be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities. If markings are not present on materials and the holder believes the information to be FOUO, the holder of the material must protect it as FOUO.

At a minimum, the bottom of each individual page containing FOUO information must be marked prominently with the caveat "FOR OFFICIAL USE ONLY." Materials containing specific types of FOUO are further marked with the applicable caveat (e.g., "LAW ENFORCEMENT SENSITIVE") in order to alert the reader of the type of information conveyed.

Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator must cite additional access and dissemination restrictions. For example:

> ***WARNING:*** *This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.*

Materials being transmitted to non-DHS recipients (e.g., other Federal agencies, state or local officials, etc.), who may not be aware of what the FOUO caveat represents, must include the following additional notice:

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.*

Computer storage media (e.g., disks, tapes, removable drives, etc.) containing FOUO information must be marked "FOR OFFICIAL USE ONLY."

Portions of a classified document, including subjects, titles, paragraphs, and subparagraphs, that contain only FOUO information must be marked "(FOUO)." Individual portion markings are not required on documents that contain no other designations.

10.5. Handling Procedures

When removed from an authorized storage location where persons without a need to know are present, or where casual observation would reveal FOUO information to unauthorized persons, an FOUO cover sheet must be used to prevent unauthorized or inadvertent disclosure.

When forwarding FOUO information, an FOUO cover sheet must be placed on top of the transmittal letter, memorandum, or document.

When receiving FOUO equivalent information from another government agency, the information must be handled in accordance with the guidance provided from the other agency. Where no guidance is provided, the information must be handled in accordance with DHS requirements.

Certain types of FOUO information are more sensitive than others based on the repercussions that could result from unauthorized or inadvertent disclosure. Such information may warrant additional safeguarding measures beyond the minimum established in this handbook. Additional control requirements must be added as necessary to afford appropriate protection to the information. Employees must evaluate risks, vulnerabilities, and potential damage to personnel or property when determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

10.6. Dissemination and Access

Access to FOUO information is based on a need to know as determined by the holder of the information. Where there is uncertainty as to a person's need to know, the holder of the information must request dissemination instructions from the information's originator or the holder's next-level supervisor. A security clearance is not required for access to FOUO information. FOUO must not be disseminated in any manner – orally, visually, or electronically – to unauthorized personnel.

The holder of the information must comply with any access and dissemination restrictions. If the information belongs to another agency or organization, the holder must comply with that agency's policy concerning access and dissemination.

When discussing or transferring FOUO information to another individual, the holder must ensure that the individual with whom the discussion is to be held or to whom the information is to be transferred has a valid need to know. Precautions must be taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

FOUO information may be shared with other agencies, Federal, state, local, or tribal government and law enforcement officials provided a specific need to know has been established and the information is shared in furtherance of a coordinated and official government activity.

10.7. Transmission

Within the United States and its territories, FOUO materials must be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container must bear the complete name and address of the sender and intended recipient, to include program office.

FOUO information may be sent by U.S. Postal Service First Class mail or an accountable commercial delivery service and may be entered into an inter-office mail system provided the information is sufficiently protected to prevent unauthorized access (e.g., sealed in an opaque envelope).

When an overseas office is serviced by a military postal facility, FOUO may be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the materials must be sent through the Department of State, Diplomatic Courier.

10.7.1. Electronic Transmission of FOUO

(a) Transmittal via Fax

Unless otherwise restricted by the originator, FOUO information may be sent via non-secure fax. However, the use of a secure fax machine is highly encouraged. Where a non-secure fax is used, the sender must coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material must comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.

(b) Transmittal via Email

FOUO information transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, FOUO may be transmitted over regular email channels. For added security, when transmitting FOUO over a regular email channel, the information can be included as a password-protected attachment with the password provided separately. Recipients of FOUO information must comply with any email restrictions imposed by the originator.

Due to inherent vulnerabilities, FOUO information must not be sent to personal email accounts, per the CBP Information Systems Security Policies and Procedures Handbook, HB 1400-05D.

10.8. Storage

When unattended, FOUO material must, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment, or similar locked compartment. An FOUO cover sheet should be used when information is removed from storage.

FOUO information must not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When FOUO materials are stored in the same container as classified materials, they must be segregated from the classified materials to the extent possible (e.g., separate folders, separate drawers, etc.).

Information technology (IT) systems that store FOUO information must be certified and accredited for operation in accordance with Federal and DHS standards. Refer to the CBP Information Systems Security Policies and Procedures Handbook, HB 1400-05D, for additional information.

10.9. Destruction

When FOUO information is no longer needed, holders of the information must destroy it in a manner to prevent recognition and reconstruction. Documents containing FOUO must be destroyed by shredding, burning, pulping, or pulverizing, after which the materials may be disposed of with normal waste.

Electronic storage media containing FOUO information must be sanitized appropriately by overwriting or degaussing. IT security personnel should be consulted for additional guidance.

10.10. Incident Reporting

The loss, suspected compromise, or unauthorized disclosure of FOUO information must be reported to the Office of Professional Responsibility, Security Management Division; the Joint Intake Center; and, if in electronic format, to the CBP Computer Security Incident Response Center. Security incidents must be reported promptly, but no later than 24 hours after the time of discovery. For additional guidance on security violations and infractions, refer to Chapter 8 of this handbook.

11. Sensitive Security Information

As defined in 49 C.F.R. § 1520.5, Sensitive Security Information (SSI) is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Transportation Security Administration (TSA) has determined would be detrimental to the security of transportation.

DHS Management Directive (MD) 11056.1, *Sensitive Security Information (SSI)*, establishes DHS policy for the recognition, identification, and overall safeguarding of SSI. For additional guidance on SSI, refer to DHS MD 11056.1 and CBP's *Sensitive Security Information Identification and Marking Guide*.

DHS MD 11056.1 establishes the TSA SSI Office as the office responsible for implementation, management, and oversight of the SSI Program within DHS and its components. Per DHS MD 11056.1, the TSA SSI Office develops, reviews, and approves department-wide policy and procedural guidance.

DHS MD 11056.1 also establishes a requirement for each DHS component to appoint an SSI Program Manager, who is responsible for the management, implementation, and oversight of SSI within the component. The CBP SSI Program Office, led by the CBP SSI Program Manager, exists within the Office of Professional Responsibility (OPR), Security Management Division (SMD). The CBP SSI Program Manager represents CBP on the DHS SSI Oversight Committee and oversees the program within CBP by providing guidance and training on SSI to CBP personnel.

11.1. DHS SSI Oversight Committee

The DHS SSI Oversight Committee is chaired by the Director of the TSA SSI Office, with membership consisting of the DHS Chief Security Officer and component SSI Program Managers. The committee is used as a forum for the discussion and development of policies and procedures related to the implementation, management, and oversight of SSI within DHS, as well as the exchange of information related to lessons learned and best practices.

11.2. Categories of SSI

The SSI Regulation (49 C.F.R. § 1520.5(b)) identifies 16 categories of information that constitutes SSI. The final category (49 C.F.R. § 1520.5(b)(16)) requires original designation authority, which is held by the Assistant Secretary for Transportation Security (hereinafter, TSA Administrator), or designee. See section 11.3.1 of this handbook for information on original designation of SSI.

Refer to the SSI Regulation (49 C.F.R. § 1520.5(b)) for the full list of categories of information and records which constitute SSI.

11.3. Identification of SSI

CBP covered persons are authorized to identify information as SSI if it meets the criteria for SSI as cited in 49 C.F.R. § 1520.5(b)(1) through (15) and implementing guidance. CBP personnel are responsible for using all available resources when identifying SSI, including TSA and CBP SSI identification guides. CBP's *Sensitive Security Information Identification and Marking Guide* provides detailed guidance and instructions for identifying CBP information and assets as SSI. Personnel should also consult with their

office's SSI Coordinator or the CBP SSI Program Manager for assistance when determining whether the information is or is not SSI.

11.3.1. Original Designation of SSI

Information that would be detrimental to the security of transportation if publicly disclosed, but that is not covered as SSI under 49 C.F.R. § 1520.5(b)(1) through (15), requires original designation by an authorized official. Within DHS, the TSA Administrator, or designee, is authorized to originally designate new types of SSI under 49 C.F.R. § 1520.5(b)(16). Additionally, detailed information about the locations at which particular screening methods or equipment are used is also SSI under 49 C.F.R. § 1520.5(b)(9)(iii) only if determined to be SSI by the TSA Administrator, or designee. No other officials within DHS have the authority to designate information as SSI that is not otherwise covered under 49 C.F.R. § 1520.5(b)(1) through (15).

Requests for original SSI designation under 49 C.F.R. § 1520.5(b)(16) must be submitted through the CBP SSI Program Manager to the Director of the TSA SSI Office for review and determination as to whether the information warrants protection as SSI. Such information must be marked and protected as SSI on an interim basis in accordance with policies and procedures issued or approved by the TSA SSI Office, pending a final assessment by the Director of the TSA SSI Office.

(a) If the Director of the TSA SSI Office concludes that the information may be eligible for protection as SSI, the TSA SSI Office will coordinate review and determination by the TSA Administrator, or designee.

(b) If the Director of the TSA SSI Office concludes that the information does not warrant protection as SSI, the information may not continue to be marked as SSI. In such cases, the CBP SSI Program Manager may request TSA SSI Office support in elevating the request for designation to the TSA Administrator, or designee.

11.4. Marking SSI

The originator of a record containing SSI is responsible for appropriately marking the information in accordance with 49 C.F.R. § 1520.13. However, all covered persons who access information believed to contain SSI are responsible for protecting and properly marking the information as SSI, whether or not they created the record.

Records containing SSI must be marked by placing the SSI header and footer conspicuously on each page of the document, including the front and back covers and any title page.

Header: SENSITIVE SECURITY INFORMATION

Footer: *WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. Parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. Parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. Parts 15 and 1520.*

11.5. Duration of SSI

Information designated or appropriately marked as SSI will remain SSI unless determined releasable by the TSA Administrator, the Commandant of the U.S. Coast Guard, the Director of the TSA SSI Office, or other authorized officials, in accordance with 49 C.F.R. § 1520.5(c) and policies and procedures issued or approved by the TSA SSI Office.

SSI that is over three years old may be subject to release upon request, unless the TSA SSI Office or the CBP SSI Program Office determines that the information requires continued protection as SSI in accordance with DHS MD 11056.1. CBP personnel must submit such requests to the CBP SSI Program Manager for official review and determination prior to release of the information, as described in section 11.6 of this handbook.

11.6. SSI Reviews

SSI reviews are conducted to identify and mark the SSI within a record. The review process is conducted to avoid both over-marking and improperly releasing SSI.

The CBP SSI Program Office will review SSI records upon request for public release under the Freedom of Information Act (FOIA), in accordance with policies and procedures issued or approved by the Director of the TSA SSI Office and section 11.13 of this handbook. CBP SSI Coordinators are authorized to conduct initial SSI reviews, and the CBP SSI Program Office must conduct a final review prior to any release.

The CBP SSI Program Office may also review SSI records in response to other requests, in accordance with DHS MD 11056.1 and policies and procedures issued or approved by the Director of the TSA SSI Office.

Information submitted for review must be marked and protected as SSI on an interim basis in accordance with policies and procedures issued or approved by the TSA SSI Office, pending a final review by the CBP SSI Program Office. (Note: Documents and reports being reviewed in preparation for release to Congress must also be portion marked for SSI at the paragraph level prior to the record's release to Congress. The portion marking for SSI is (SSI).)

11.7. SSI Challenges

Any authorized holder of SSI who believes that information has been improperly or erroneously marked as SSI is encouraged to challenge the marking. Such challenges may be processed either (1) informally, by contacting the person who originally designated the information as SSI, or (2) formally, by submitting an SSI challenge request in writing to the CBP SSI Program Office, which will coordinate the request with the TSA SSI Office. Refer to the DHS MD 11056.1 for additional information on SSI challenges and appeals.

11.8. Compliance Reviews and Self-Inspections

As the CBP SSI Program Office, OPR/SMD will conduct periodic oversight and compliance reviews of SSI within CBP as deemed appropriate.

Self-inspections assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding. The CBP SSI Program

Manager conducts a self-inspection of CBP's SSI Program at least once every 18 months. CBP SSI coordinators are responsible for conducting self-inspections of their offices' SSI programs at least once every 12 months. The results of self-inspections must be reported to the CBP SSI Program Office within 30 days of completion. Discrepancies cited during self-inspections must be reconciled within 45 work days, and the CBP SSI Coordinator or the CBP SSI Program Manager will take remedial action as needed.

11.9. Access and Dissemination

SSI must not be disseminated in any manner (i.e., orally, electronically, visually, or in any other manner) to unauthorized individuals. The TSA Administrator may determine in writing that information which might otherwise be considered SSI may be released publicly in the interest of public safety or in furtherance of transportation security in accordance with policies and procedures issued or approved by the TSA SSI Office.

Access to SSI is based on an individual's status as a covered person with a legitimate need to know the SSI, as determined by the holder of the information.

A covered person is an individual or entity that has transportation security or transportation security-related responsibilities including, but not limited to:

(a) Anyone who is permanently or temporarily assigned to, attached to, detailed to, employed by, or under contract with DHS;

(b) Regulated parties, Federal, state, local, and tribal government employees, contractors, and grantees;

(c) Committees of Congress;

(d) Other persons with a need to know as defined in 49 C.F.R. § 1520.11; and

(e) Persons receiving SSI pursuant to other conditional disclosures.

CBP employees have a need to know SSI if access to the information is necessary for the performance of their official duties. Where there is uncertainty as to a person's need to know, the holder of the information must request dissemination instructions from his or her next-level supervisor or the originator of the information.

A security clearance is not required for access to SSI. However, with approval from the TSA SSI Office, CBP may make an individual's access to SSI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding SSI. For more information on determining if an individual is a covered person with a need to know, contact the CBP SSI Program Office.

11.10. Storage and Handling

Personnel who possess records containing SSI are responsible for ensuring that those records are properly protected to prevent unauthorized or inadvertent disclosure. When not under a covered person's direct physical control, SSI records and materials must, at a minimum, be stored in a locked container, desk drawer, cabinet or office.

When SSI is removed from an authorized storage location where non-covered persons or covered persons without a need to know are present, or where casual observation

could reveal SSI to unauthorized individuals, measures must be taken to protect the SSI from unauthorized or inadvertent disclosure, such as placing the SSI in an opaque envelope or folder or attaching an SSI cover sheet to document.

11.11. Transmission

When discussing or transmitting SSI to another individual, CBP personnel must ensure that the individual with whom the discussion is to be held or to whom the information is to be transferred is a covered person with a valid need to know. Personnel must take precautions to prevent unauthorized individuals from overhearing a conversation containing SSI and be cognizant of their surroundings when discussing SSI over the telephone.

Reasonable precautions must be taken when hand-carrying or mailing SSI to minimize the risk of loss or improper disclosure. SSI records must be packaged in an opaque envelope or other similar wrapping that affords sufficient protection to prevent unauthorized access, and sealed in a manner that prevents inadvertent opening and shows evidence of tampering. The outer packaging must not be marked as SSI. When hand-delivering SSI, the material must be personally delivered to the intended recipient; SSI must never be left unattended in a recipient's workspace. SSI must be mailed by U.S. First Class mail or other traceable delivery service.

SSI may be placed into an inter-office mail system provided the information is sufficiently protected to prevent unauthorized access (i.e., contained within a sealed envelope).

11.11.1. Electronic Transmission

Records containing SSI must be encrypted within all email, even within DHS, as well as when sent by other methods of electronic transmission outside of DHS. When emailing SSI, the SSI must always be contained in a password-protected attachment; SSI must never be placed in the body of an email. The password must be provided in a separate email without any identifying information (i.e., no subject line or email content) or by phone. Passwords used to encrypt records containing SSI must meet specific criteria identified by the TSA SSI Office. All passwords must:

(a) Be at least eight characters in length;

(b) Have at least one upper-case and one lower-case letter;

(c) Contain at least one number;

(d) Contain at least one symbol (e.g., !@#$%^&*); and

(e) Not be a word in the dictionary.

SSI must not be posted to any publicly accessible website or to any DHS or CBP intranet site that is not authenticated and restricted to covered persons with a need to know.

Personnel may send records containing SSI via fax provided an SSI fax cover sheet is attached to the front of the document, the fax number is verified to be current and correct, and the recipient is standing by to receive the faxed record.

11.12. Destruction

SSI must be destroyed when it is no longer needed and when its continued retention is not otherwise required under the National Archives and Records Administration (NARA) records retention laws and regulations.

Records containing SSI must be destroyed in a manner that prevents recognition or reconstruction, such as by shredding, burning, pulping, or pulverizing. After destruction, the materials may be disposed of with normal waste.

Electronic records must be deleted in accordance with policies or procedures issued or approved by the TSA SSI Office and in accordance with NARA records retention policies. Electronic storage media (e.g., CDs, DVDs, disks, etc.) must be shredded, incinerated, disintegrated, or otherwise sanitized by overwriting or degaussing. Information technology (IT) security personnel should be consulted for additional guidance.

11.13. CBP FOIA Review Process

All requests submitted to the CBP FOIA Office must be reviewed for the presence of sensitive CBP information, including SSI, in responsive material. If the CBP FOIA Office determines that a record responsive to a FOIA request may contain SSI, it must be forwarded to the CBP SSI Program Manager for a full review.

Information designated as SSI qualifies for exemption from release under FOIA. Records containing SSI may be released only after the SSI has been properly redacted from the record.

11.14. Incident Reporting

CBP personnel are responsible for reporting any incident involving the loss, compromise, unauthorized disclosure, improper transmission, mishandling, or mismarking of SSI to their immediate supervisor and the designated SSI Coordinator. The SSI Coordinator must report the incident to the CBP SSI Program Office (OPR/SMD) promptly, but no later than the next business day after discovery. Upon receiving an SSI incident report, the CBP SSI Program Office reviews the information to confirm whether the record contains SSI and to determine the level of compromise or potential compromise resulting from the incident.

In the event of a major SSI incident, the CBP SSI Program Office will coordinate incident resolution with the TSA SSI Office and, if applicable, with the CBP Computer Security Incident Response Center, in accordance with IT incident reporting requirements. Major SSI incidents involve the loss, breach, or unauthorized disclosure of SSI to non-covered persons or to covered persons without a need to know, or the failure to apply proper safeguarding measures when electronically transmitting SSI (e.g., SSI password incidents).

CBP adheres to procedures established by the TSA SSI Office in coordination with the DHS SSI Oversight Committee for reporting, mitigating, and investigating incidents involving the improper handling or unauthorized disclosure of SSI.

12. Security Education, Training, and Awareness

A security program is most effective when employees practice security daily. The Office of Professional Responsibility (OPR), Security Management Division (SMD) is responsible for Security Education, Training, and Awareness as it pertains to administrative security (i.e., safeguarding of classified and sensitive but unclassified information), physical security, and operations security. CBP personnel who have not fulfilled the mandatory training requirements may be restricted from accessing classified information until the requirements are met.

12.1. Security Training

Security training encompasses the fundamentals of how to properly safeguard classified and sensitive but unclassified information. The overall intent of training is to provide CBP personnel with the basic knowledge required to work effectively with critical information. The goals of the Security Education, Training, and Awareness program are to ensure that each employee who creates, processes, or handles classified information has satisfactory knowledge and understanding of classification, safeguarding, and declassification policies, procedures, and practices; to increase uniformity among personnel when handling classified and sensitive but unclassified information; to reduce the possibility of improper classification, safeguarding, and transmission; and to ensure that security incidents are promptly reported.

Training includes a variety of delivery methods, including Web-based instruction and instructor-led briefings provided by OPR/SMD or a security liaison.

In accordance with DHS Instruction 121-01-011, Chapter 10 (Security Education, Training, and Awareness Program), the CBP Security Education, Training, and Awareness program includes, but is not limited to, the development and presentation of the following mandatory trainings:

(a) Security Orientation Briefing

All CBP employees, contractors, consultants, and detailed personnel are required to attend a Security Orientation Briefing within the first 30 days of assignment. It is only necessary to attend Security Orientation one time.

(b) Initial Security Briefing

An initial security briefing is provided to all CBP personnel who have met the requirements for access to classified information. Prior to being granted access to classified information, individuals receive a comprehensive briefing to inform them of the basic security policies, principles, practices, and criminal, civil, and administrative penalties. At that time, individuals execute an SF-312 (Classified Information Nondisclosure Agreement). The signed SF-312 is witnessed by the individual conducting the briefing and submitted to the OPR Personnel Security Division (PSD) for filing in the individual's permanent personnel security file. An individual is only required to sign an SF-312 one time unless he or she has been debriefed or his or her clearance has been administratively withdrawn, in which case the individual receives another briefing and a new SF-312 is signed prior to receiving access.

(c) Annual Refresher Training

Annual refresher briefings are mandatory for all personnel to reinforce and update awareness of security policies and responsibilities. All CBP personnel must complete the annual CBP Safeguarding Classified National Security Information training on the DHS Performance and Learning Management System (DHS PALMS). Annual refresher training addresses the identification and handling of other agency-originated information and foreign government information, the threat of foreign intelligence activities attempting to obtain classified information, the techniques employed by foreign intelligence activities to gain classified information, and the penalties for engaging in espionage activities.

(d) Termination Briefings

Individuals must receive termination briefings to inform them of their continuing security responsibilities after their access authorizations are terminated. A termination briefing is provided on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified information. The termination briefing is conducted by the individual's supervisor or by personnel from OPR/PSD, and the acknowledgement statement becomes part of the individual's permanent personnel security file.

(e) Original Classification Authority (OCA) Training

OCAs must receive training in proper classification and declassification with an emphasis on the avoidance of over-classification. At a minimum, the training covers classification standards, classification levels, classification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing. This training is provided prior to the individual originally classifying information and at least once each calendar year thereafter. OCAs who do not receive this mandatory training at least once within a calendar year have their classification authority suspended until such training has taken place, unless a temporary waiver has been approved. OCAs sign an acknowledgement at the completion of the training session.

(f) Derivative Classification and Marking Training

Persons who may apply derivative classification markings, regardless of media, and persons who have access to any classified system (e.g., Homeland Secure Data Network (HSDN) and/or Joint Worldwide Intelligence Communications System (JWICS) accounts) must receive training and be certified prior to taking any derivative classification action. Training includes the proper application of the derivative classification principles, the avoidance of over-classification and, at a minimum, the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing. In addition to this preparatory training, derivative classifiers are required to receive such training at least once every two years. Derivative classifiers who do not receive this mandatory training at least once every two years have their authority to

apply derivative classification markings suspended until they have received the proper training unless a temporary waiver is granted.

(g) Other Specialized Training

Classification management specialists, security managers, security specialists, declassification authorities, and all other personnel whose duties significantly involve the creation or handling of classified information may receive more detailed or additional training no later than six months after assumption of duties that require other specialized training.

Training topics may include, but are not limited to, the overview of DHS safeguards and security disciplines, such as personnel security, information security, protection of government property, locks and containers, risk management reporting and notification requirements, legal and administrative sanctions imposed for incurring a security violation, construction security, Sensitive Compartmented Information Facility construction, and/or foreign intelligence service threats to sensitive and classified information.

13. North Atlantic Treaty Organization (NATO) Information

This chapter sets forth CBP's policy regarding the safeguarding of NATO information. Classified NATO information is information that represents military, political, and economic data circulated within NATO, including information received from member nations as well as information originated within the organization itself. The protection of this information is controlled under the NATO security regulations, and access is determined by the holder, unless restrictions are specified by the originator at the time of release to NATO.

Material received by CBP directly from another NATO member nation may contain either NATO information generated by a NATO element or national information generated by a NATO member nation. If it has been marked "NATO" by the originating nation, it must be assumed to contain information released to NATO, and it is controlled under the NATO Security Program.

13.1. Marking

Document and portion markings are required for classified NATO information. Marking principles for NATO information are the same as for U.S. classified national security information.

(a) Cosmic Top Secret (CTS) – This security classification is applied to information, the unauthorized disclosure of which would cause exceptionally grave damage to NATO.

(b) NATO Secret (NS) – This security classification is applied to information, the unauthorized disclosure of which would cause serious damage to NATO.

(c) NATO Confidential (NC) – This security classification is applied to information, the unauthorized disclosure of which would be damaging to the interests of NATO.

(d) NATO Restricted (NR) – This security classification is applied to information, the unauthorized disclosure of which would be disadvantageous to the interests of NATO. (Note: Although the safeguards for this marking are similar to those of sensitive but unclassified information, "NATO Restricted" is a security classification.)

(e) ATOMAL – This information can be either U.S. Restricted Data or Formerly Restricted Data that is classified pursuant to the Atomic Energy Act of 1954, as amended, or United Kingdom ATOMIC information that has been officially released to NATO. ATOMAL information is marked as follows:

i. Cosmic Top Secret ATOMAL (CTSA)

ii. NATO Secret ATOMAL (NSA)

iii. NATO Confidential ATOMAL (NCA)

(f) NATO Unclassified (NU) – This marking is applied to official information that is the property of NATO, but does not meet the criteria for classification. Access to the information by non-NATO entities is permitted when such access would not be detrimental to NATO. In this regard, it is similar to U.S. government official information that must be reviewed prior to public release. NATO Unclassified information only requires portion markings when it is part of a larger document intermixing NATO classified information or non-NATO information.

13.2. Access

Access to classified NATO information is based on a demonstrated need to know, possession of the appropriate level security clearance, and receipt of a NATO security briefing provided by the Office of Professional Responsibility (OPR), Security Management Division (SMD).

(a) Access to classified NATO information above the NATO Restricted level requires a NATO clearance of at least the level of information to be accessed.

(b) Access to NATO Restricted or NATO Unclassified information does not require a clearance, but a need to know is required.

(c) Anyone accessing classified NATO information must have a NATO security briefing before initial access and an annual refresher briefing thereafter.

(d) When access to classified NATO information is no longer required, individuals will be debriefed and the record of the debriefing will be maintained for one year by OPR/SMD.

13.2.1. NATO Clearances

(a) Requests for NATO clearances, with justification, will be processed through OPR/SMD for approval.

(b) A NATO Secret or Confidential clearance requires a valid U.S. Secret clearance.

(c) Interim U.S. Secret clearances are acceptable for access to non-ATOMAL NATO Secret information and below.

(d) A Cosmic Top Secret clearance requires a final U.S. Top Secret clearance.

(e) Access to ATOMAL information requires a final U.S. Top Secret clearance, regardless of the actual level of classification.

13.3. Accountability and Control

NATO information flows down from the Central United States Registry (CUSR) to DHS users through a system of sub-registries, control points, and user offices. Sub-registries are offices that receive materials directly from the CUSR and are established by the CUSR. Control points are established through a sub-registry. User offices can be established through a sub-registry or a control point. Control points and user offices receive materials and operational guidance from their establishing office.

OPR/SMD serves as the control point for NATO information within CBP.

13.4. Storage

Cosmic Top Secret, NATO Secret, and NATO Confidential information is afforded the same level of protection given its U.S. equivalent, as described in Chapter 6 of this handbook. NATO information must be stored separately from other classified non-NATO information. A separate drawer or a partition within a drawer is sufficient to meet this requirement.

NATO Restricted information is afforded the same protection as U.S. Confidential information when possible. However, storage in a locked drawer or file cabinet is acceptable when other storage is not practical. NATO Restricted information is processed or stored only on systems approved for the processing of classified U.S. information.

NATO Unclassified information is afforded the same protections as information identified as For Official Use Only (FOUO), as described in Chapter 10 of this handbook.

Open storage of classified NATO information is afforded the same level of protection given its U.S. equivalent.

The use of cover sheets with classified NATO materials is required. Either NATO cover sheets or the equivalent U.S. Standard Form (SF) series cover sheets are acceptable.

13.5. Transmission and Transportation

Transmission and transportation of NATO Confidential, NATO Secret, and Cosmic Top Secret information is afforded the same protections as its U.S. equivalent classification with the exception of commercial overnight delivery, which is prohibited. Refer to Chapter 7 of this handbook for additional information.

Courier cards must indicate that the holder has a NATO clearance if there is a requirement to transport classified NATO information.

Except for mail, NATO Restricted materials must be transmitted or transported in a manner approved for NATO Confidential or higher information.

Transmittal of NATO Restricted information requires the use of secure phone, fax, or an email system approved for the transmission of classified U.S. information.

NATO Restricted information is sent using U.S. First Class mail. The information must be double wrapped, and the outer envelope may count as one of the wrappings. The contents or the fact that the information is NATO classified must not be discernible from the outside.

13.6. Destruction

Classified NATO information must be destroyed in the same manner approved for classified U.S. information, as described in section 5.7 of this handbook.

NATO Unclassified information may be destroyed in any manner prescribed for FOUO, as described in section 10.9 of this handbook.

Destruction certificates, signed by two properly cleared persons, are required for NATO Secret, Cosmic Top Secret, and all ATOMAL. NATO Secret certificates are maintained for 5 years and Cosmic Top Secret certificates are maintained for 10 years. Cosmic Top Secret ATOMAL certificates are maintained for 10 years, and NATO Secret ATOMAL and NATO Confidential ATOMAL are maintained for 5 years.

NATO Secret, Cosmic Top Secret, and all ATOMAL documents must be destroyed at the sub-registry, unless specifically approved for destruction at the control point level. Destruction of these documents must not be further delegated to the user office level.

13.7. Incident Reporting

The loss, suspected compromise, or unauthorized disclosure of NATO classified information must be reported to OPR/SMD, the Joint Intake Center, and, if in electronic format, to the CBP Computer Security Incident Response Center. Security incidents must be reported promptly, but no later than 24 hours after the time of discovery. For additional guidance on security violations and infractions, refer to Chapter 8 of this handbook.

14. Security Compliance Reviews and Self-Inspections

Security compliance reviews, which consist of self-inspections, security surveys, assessments, assistance visits, compliance reviews, and unannounced spot checks, are conducted to ensure compliance with laws, executive orders, Federal regulations, and DHS policies.

This chapter provides an overview of security compliance reviews conducted by the Office of Professional Responsibility (OPR), Security Management Division (SMD) and ongoing standards for the Self-Inspection Program as it relates to the safeguarding of classified and sensitive but unclassified information.

14.1. Compliance Review Procedures

The frequency of compliance reviews is based on CBP office needs, the volume of classified material produced and stored within each office, and self-inspection results.

The compliance review team will provide an in-briefing prior to the assessment to outline the nature of the review, and an exit briefing at the conclusion of the assessment to note findings.

Compliance assessments are not limited to the protection of critical information and may include personnel and operational security practices. Assessments include the following review areas:

(a) Review of internal procedures and processes for the safeguarding of classified and sensitive but unclassified information;

(b) Interviews with office personnel;

(c) Review of access and control records;

(d) Review of safes/security containers; and

(e) Review of a sampling of classified (both original and derivative classification actions) and sensitive but unclassified documents processed and/or stored at the facility.

The compliance review team will prepare a draft report that documents preliminary findings and recommendations. A final report will be provided to the relevant CBP program activity through the appropriate CBP office head (i.e., Assistant Commissioner).

14.2. Self-Inspections

CBP offices are required to conduct annual self-inspections to assess the safeguarding of classified and sensitive but unclassified information. OPR/SMD receives and analyzes self-inspection results and will follow up with program offices where deficiencies are identified.

14.3. Unannounced Reviews

OPR/SMD may conduct unannounced reviews of CBP offices without the benefit of advance notification. An unannounced review is conducted when issues or circumstances arise, which raise concerns relative to the effective and efficient management of classified or sensitive but unclassified information within a CBP office, or upon request by the CBP office head.

14.4. External Reviews and Inspections

CBP offices are subject to reviews and inspections from outside entities, such as the DHS Chief Security Office, DHS Office of Inspector General, and the National Archives Records Administration, Information Security Oversight Office.

Appendix A. Classified Meeting Procedures Checklist

The steps listed on this checklist must be completed prior to, during, and after a classified meeting to reduce the risk of unauthorized disclosure of classified information.

Before the meeting

Prior to occupying the conference room, the host or Designated Security Officer (DSO) must:

- ☐ Disable all electronic equipment capable of transmitting signals outside of the room by:
  - ☐ Switching off the media system
  - ☐ Unplugging the power cord from the wall
  - ☐ Unplugging any other cables from the wall (e.g., phone lines, Ethernet cables, etc.)
- ☐ Remove or unplug all telephones within the room
- ☐ Remove trash cans from the room
- ☐ Ensure the white noise generator is operating, if applicable
- ☐ Conduct a sound attenuation test to ensure normal conversation inside the room cannot be heard intelligibly outside the room, paying particular attention to vents, ducts, doorways, and other openings
- ☐ Establish a "secure" area around the room by posting cleared host personnel at doors and hallways to keep the room's perimeter under surveillance, to prevent passers-by from listening, and to control access by using the list of invitees as an access roster and verifying attendees using their photo identification
- ☐ Ensure attendees' security clearances are equal to or higher than the classification level of the information to be disclosed during the meeting (Note: For more information about security clearance verification, refer to the CBP Information Security Handbook, HB 1400-04, Section 4.2.)
- ☐ Enforce the "no wireless devices allowed" rule and remind attendees of this rule in advance
  - ☐ Provide a suitable location outside of the conference room for attendees to relinquish their Portable Electronic Devices (PEDs), which should be guarded by the host staff (Examples of PEDs include, but are not limited to, laptops, thumb drives, mobile phones and devices, smartwatches, activity trackers, or any device that is capable of capturing or transmitting data, videos, images, or recordings.)
- ☐ Notify each attendee and presenter of:
  - ☐ The highest level of classified information to be presented/discussed
  - ☐ The specific classification or unclassified status of each presentation (when multiple presentations will be given)
  - ☐ Limitations associated with classified portions of the meeting (e.g., note taking)
- ☐ Escort those who do not have the appropriate level security clearance from the room

During the meeting

During the meeting, the host or DSO must:

- ☐ Ensure that an authorized person from the host office remains in the conference room to observe and assist attendees in avoiding information security incidents (e.g., accidentally placing working notes in their bag)
- ☐ Ensure that attendees' voices do not rise above the white noise generator
- ☐ When necessary, permit only accredited classified laptops without network connections to be attached to the projector
- ☐ Have a procedure or plan in place to grant or deny access when an attendee arrives late to the meeting
- ☐ Ensure than an authorized person remains in the room during breaks when classified information is present

After the meeting

Immediately upon the conclusion of the meeting, the host or DSO must:

- ☐ If there is a need for attendees to transport classified materials back to their offices, verify that they possess a valid courier card or courier authorization letter. Attendees without a valid courier card or courier authorization letter may coordinate the mailing of the classified information in accordance with established procedures
- ☐ Provide materials to properly double-wrap any classified information distributed during the meeting (as appropriate for the level of classification) so that attendees may hand-carry material back to their offices, if appropriate
- ☐ Conduct a "sweep" of the conference room and adjacent areas to ensure classified or sensitive materials have not been left behind
- ☐ Ensure excess classified information is properly safeguarded or destroyed

Appendix B. Sample Emergency Action Plan

Instructions for use: *In accordance with DHS policy, each program office that handles or stores classified material must prepare a plan for the protection and destruction of classified information in the event of an emergency. Below is a standard sample plan that comprises the basic required elements and may be modified or customized for the individual program office to which it applies.*

The final emergency action plan must be distributed to all cleared personnel within the applicable program office, and personnel must be briefed on their responsibilities as defined within the plan.

Purpose

To establish procedures for the protection, removal, or destruction of classified material in case of an emergency, such as a fire, natural disaster, civil disturbance, terrorist event, hostile action, or unexpected and immediate evacuation of office space, to minimize the risk of compromise. Although the importance of protecting classified material cannot be discounted, it must be accomplished in such a way as to minimize the risk of loss of life or injury to employees.

Applicability

This emergency action plan applies to personnel, contractors, and detailees assigned within (*office or program name*).

Authorities/References

- DHS Instruction 121-01-011, *The Department of Homeland Security Administrative Security Program*

Responsibilities

- The (*position title of office or program head*) is responsible for the oversight of the emergency action plan.
- The (*position title of senior security representative*) is responsible for implementation of the emergency action plan for the protection of classified material and will ensure precautions are taken to prevent the loss or compromise of such material in the event of an emergency.
- All (*office or program*) personnel are responsible for adhering to the procedures specified in the emergency action plan and for taking appropriate actions to ensure the safeguarding of classified material in the event of an emergency.

Procedures

1. If there is no imminent danger to employees:
    1.1. Immediately check all workspaces for unsecured classified material and return it to the classified storage area or authorized storage containers before evacuation.
    1.2. If authorized storage containers are not immediately available, attempt to remove the classified material from the area, seeking assistance from other properly cleared personnel. In doing so, take necessary precautions to ensure inadvertent disclosure

does not occur. Continue to safeguard the material until it can be secured in an approved container at another nearby CBP or DHS facility.

2. If there is imminent danger to employees:

   2.1. Evacuate immediately, leaving classified material in place. Under no circumstances should employees risk their own safety or the safety of others while attempting to secure or remove classified material from workspaces.

   2.2. Immediately report the existence of unattended classified material to the senior security representative present. Identify the level of classification and subject of material left unattended, if known.

   2.3. The senior security representative will designate personnel to monitor the area perimeter and note any unauthorized access to the area.

   2.4. Upon resolution of the emergency situation, and when permitted to do so, authorized personnel will survey all controlled spaces, security containers, strong rooms, and vaults for evidence of forced entry and immediately inventory all classified material. Any irregularities will be reported to the senior security representative present.

3. In the event the emergency destruction of classified material is necessary:

   3.1. Destruction will be authorized by the senior security representative present.

   3.2. When possible, classified material will be destroyed using equipment previously authorized for classified destruction and in accordance with applicable policies.

   3.3. When such equipment is not available, or circumstances dictate otherwise, classified material will be destroyed by any means that will ensure positive destruction and preclude recognition or reconstruction of the material.

   3.4. Document control cover sheets, if attached, will be removed prior to destruction and delivered to the senior security representative present as a record of destruction.

   3.5. A record for documents that do not have control cover sheets and are classified Top Secret, NATO Secret, or ATOMAL will be completed, identifying at a minimum the control number, classification, and subject. The names of personnel completing the destruction and any witnesses will also be documented.

4. In the event that circumstances warrant the destruction of all classified material, the material will be destroyed based on the following priorities:

   - Priority 1 – Top Secret, COSMIC Top Secret, Top Secret ATOMAL
   - Priority 2 – Secret, NATO Secret, NATO Secret ATOMAL
   - Priority 3 – Confidential, NATO Confidential, NATO Confidential ATOMAL
   - Priority 4 – Sensitive But Unclassified (Sensitive Security Information, For Official Use Only)

A copy of this document must be filed as the first document in any safe containing classified material. In multiple drawer safes with only one lock, this document must be filed as the first document in the top drawer. Safes that have multiple drawers and multiple locks must have a copy of this document filed as the first document in each drawer.

Appendix C. Responsibilities of the Designated Security Officer

CBP offices that handle or store classified information/material must appoint, in writing, a Designated Security Officer (DSO) and provide the name of the appointed DSO to the Office of Professional Responsibility (OPR), Security Management Division (SMD). One primary and one alternate DSO must be appointed for each sector, field office, air and marine location, and program office.

1. The DSO is required to complete the CBP Safeguarding Classified National Security Information and the Sensitive Security Information trainings located on the DHS Performance and Learning Management System (DHS PALMS). The Safeguarding Sensitive But Unclassified Information training will be provided by OPR/SMD electronically.

2. The DSO provides guidance to CBP personnel within his or her area of responsibility on the protection of classified and sensitive but unclassified information, as needed, to support the initial training provided by OPR/SMD.

3. The DSO is responsible for tracking combination changes and lock maintenance of security containers by the Classified Document Custodians (CDC) within his or her respective operational or program office. This responsibility includes:

   (a) Ensuring that combinations are changed in accordance with applicable DHS and CBP policies;

   (b) Ensuring that CDCs record combination changes for security containers on the SF-700 (Security Container Information), which must be stored at the nearest CBP office with an approved classified storage container;

   (c) Verifying that the individuals listed on the SF-700 have the appropriate security clearance; and

   (d) Ensuring that CDCs update the Classified Storage Container database maintained by OPR/SMD when a container is no longer used for the storage of classified information.

4. The DSO is responsible for ensuring that the CDC perform an annual inventory on all security containers for which the CDC is responsible by September 30 of every year (once each fiscal year). The DSO must collect results of the inventory, including any findings, from the CDC.

5. The DSO must work with the CDC to develop and implement a communications plan for reporting possible security incidents and inefficient security practices to OPR/SMD. The DSO must immediately notify OPR/SMD of any incident involving the loss or compromise of classified or sensitive but unclassified information.

6. The DSO must develop and implement a local security inspection program and ensure that established DHS and CBP information security requirements are followed.

7. Upon notification from OPR/SMD, the DSO is responsible for the collection of data required for the SF-311 (Agency Security Classification Management Program Data) and the Cost Estimate Report, which is submitted to OPR/SMD annually.

8. The DSO serves as the liaison for courier card requests.

(a) Upon receipt of a DHS Form 11000-2 (Courier Authorization Request), the DSO must verify that all sections of the form are completed accurately.

(b) The DSO must verify that the form has been signed by the appropriate authorizing official and that a legitimate justification is provided. The DSO submits the form to OPR/SMD for processing.

(c) The DSO must retain the original DHS Form 11000-2 for classified couriers within his or her area of responsibility.

(d) The DSO must ensure that each classified courier receives a copy of the *Guidance for Classified Couriers* briefing pamphlet and signs a form acknowledging receipt of his or her courier card. (Note: OPR/SMD no longer maintains copies of signed courier acknowledgement receipts.)

Appendix D. Responsibilities of the Classified Document Custodian

CBP offices that store classified material must appoint, in writing, a Classified Document Custodian (CDC) and provide the name of the appointed representative to the appropriate Designated Security Officer (DSO). More than one CDC may be appointed for each CBP office.

1. The CDC is required to complete the CBP Safeguarding Classified National Security Information training located on the DHS Performance and Learning Management System (DHS PALMS). In addition, it is suggested that the CDC complete the DHS Lock and Containers course, which is provided by the Security Training Branch of the DHS Office of the Chief Security Officer, Administrative Security Division.

2. The CDC is responsible for the security container(s) located in his or her respective office.

3. The CDC must maintain receipts for classified material transferred outside of CBP by his or her office. For more information regarding receipts for classified information transmission, please refer to the CBP Information Security Handbook, HB 1400-04, Section 5.5.

4. The CDC is required to perform an annual inventory of classified material stored in the security container(s) located in his or her office by September 30 of every year (once each fiscal year). The CDC must report the results of the inventory, including any findings, to the DSO.

5. The CDC must establish a system of security checks to be completed at the end of each work day to ensure that the area is secure and that classified information has been properly stored.

6. The CDC is responsible for ensuring the SF-700 (Security Container Information) and SF-702 (Security Container Check Sheet) are completed in accordance with DHS and CBP requirements. The CDC must verify that individuals listed on the SF-700 have the appropriate security clearance. When a security container is no longer used for the storage of classified information, the CDC must update the Classified Storage Container database maintained by the Office of Professional Responsibility (OPR), Security Management Division (SMD).

7. CBP facilities located within the National Capital Region must complete SF-700, Part 2 and provide it to OPR/SMD for storage purposes.

8. CBP facilities located outside of the National Capital Region must forward the completed SF-700, Part 2 to the nearest CBP office with an approved classified storage container.

9. The CDC must ensure that destruction of classified information is completed in accordance with established DHS and CBP policies.

10. The CDC is responsible for ensuring that appropriate security measures are taken when reproducing classified material, in accordance with DHS and CBP requirements.

11. The CDC is responsible for completing a Classified Storage Container/Room Form in the Classified Storage Container database for each security container that is used to store classified information within his or her respective office.

Appendix E. Security Container Turnover Procedures

Purpose

The purpose of the security container turnover process is to identify and properly destroy any classified materials that are no longer required for a CBP office's programs and operations, following the resignation, transfer, or other departure of a senior CBP official. The process is also required to ensure that only materials classified at or below the highest level of classification authorized for storage are contained in the security container to which the senior CBP official had access. The proper storage of classified information is critical to prevent unauthorized or inadvertent disclosure to individuals without adequate clearance or need to know.

Applicability

The procedures and requirements described in this document apply to CBP personnel who are authorized to access a classified security container, to which a senior CBP official is also authorized access. (Note: This guidance does not apply to safes used for communications security (COMSEC) equipment or to security containers located in a Sensitive Compartmented Information Facility.)

Authorities

- DHS Instruction 121-01-011, *The Department of Homeland Security Administrative Security Program.*
- CBP HB 1400-04, *Information Security Handbook*, September 2015.

Definitions

- For the purpose of this document, a **senior CBP official** is defined as any CBP employee serving in a GS-15 level position or a Senior Executive Service position.
- An **authorized official** refers to a CBP employee who is authorized to access the classified security container(s) to which the exiting senior CBP official also had access. The authorized official may be one of the employees listed on the SF-700 and/or the Classified Document Custodian (CDC) responsible for the security container(s) to be reviewed.

Requirements

- When an event involving the resignation, transfer, or other departure of a senior CBP official occurs, an authorized official must conduct an inventory and turnover of the contents of all classified security containers to which the senior official had access during his or her tenure in the position being vacated. This review is a required turnover procedure to ensure compliance with established policy for the proper storage of classified national security information.
- The security container inventory and turnover process must take place within three (3) business days following departure of the senior CBP official.
- If conducted by the CDC, this inventory may also serve the purpose of the required annual security container inventory. For more information about the annual inventory requirement for CBP, refer to the CBP Information Security Handbook, HB 1400-04, Section 6.11.

Procedures (*Security Container Review Process*)

1. Turnover Review

1.1. The authorized official must review all classified materials and documents stored within the security container to assess the information's continued applicability to the office's program activities and operations.

1.2. Classified documents that are determined to be relevant to the office's current or future operations may continue to be retained in the security container.

1.3. Classified documents that are determined to be obsolete or no longer needed in support of the office's ongoing operations must be removed from the security container and identified for destruction.

1.3.1. Any classified material that has been identified for destruction must continue to be protected, as appropriate for its classification level, until it is actually destroyed.

1.3.2. Classified information identified for destruction must be destroyed completely to preclude recognition or reconstruction of the classified information. Methods and equipment approved for destroying classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition, or pulverizing. Please refer to the CBP Information Security Handbook, HB 1400-04, Section 5.7, for more information regarding the destruction of classified material.

2. Compliance Review

2.1. To ensure proper storage of classified information, the authorized official must review each page of every document stored within the security container, including pages attached by staples or paper clips. For guidance on the proper storage of classified national security information, please refer to the CBP Information Security Handbook, HB 1400-04, Chapter 6.

2.2. The authorized official must look at the classification markings (both overall and portion markings) on each page of every document to ensure the material is appropriate for storage in the security container.

2.2.1. Example: A classified storage container approved at the SECRET level may contain materials up to and including collateral SECRET classified information; however, collateral classified information above SECRET (e.g., TOP SECRET) or Sensitive Compartmented Information at any level is not approved for storage in a SECRET security container.

2.3. Upon completion of the review, the authorized official should replace all compliant documents back in the security container as appropriate.

2.4. If any instances of improperly stored classified information were discovered during the compliance review, the authorized official must take immediate action to report the discovery and secure the material appropriately.

2.4.1. Report any discovery of improperly stored classified information immediately to the Office of Professional Responsibility (OPR), Security Management Division (SMD) at CBP.Security@dhs.gov. OPR/SMD will provide instructions for securing the material.

3. Security Container Combination Maintenance

3.1. The resignation, transfer, or other departure of a senior CBP official qualifies as a condition that requires changing of the combination to all security containers to which the individual had access, in accordance with the 32 C.F.R. Part 2001, *Classified National Security Information; Final Rule*.

3.1.1. As such, the appropriate CDC or other authorized individual is responsible for changing the combination to the classified security container immediately upon the senior CBP official departing the position that required access.

3.1.2. A new SF-700 (Security Container Information) must be executed to record the updated combination.

3.1.3. Refer to the CBP Information Security Handbook, HB 1400-04, Section 6.7, for further guidance on security container combinations and execution of the SF-700.

4. Reporting

4.1. The authorized official must report completion of the security container turnover process and identify any noncompliant findings to the container's respective CDC (if the authorized official is different from the CDC). The CDC must in turn report completion of the review and any reported findings to the appropriate Designated Security Officer, regardless of whether the review was conducted by the CDC or another authorized official.

4.1.1. In addition to discoveries of improperly stored classified material, noncompliant findings may include:

- Failure to complete required end-of-day security checks using SF-701 (Activity Security Checklist);
- Failure to record each time the security container is opened, closed, and checked using SF-702 (Security Container Check Sheet); or
- The discovery of unauthorized items in a security container used for the storage of classified information. Such items may include, but are not limited to, weapons, sensitive or valuable items (e.g., funds, jewelry, precious metals, etc.), seized items (e.g., drugs), or personal papers and effects.

Contact

For additional information or for questions regarding security container turnover procedures, please contact the OPR/SMD at CBP.Security@dhs.gov.

Appendix F. Inadvertent Disclosure Statement

Classified national security information has been either discussed with you or exposed to your view without proper authorization. In light of this unintentional disclosure, it is necessary that you execute the statement below affirming that you will maintain the security of any properly classified information you may have gained through such disclosure.

The importance of safeguarding this classified national security information cannot be overemphasized. Any unauthorized disclosure or release of the classified information to which you have had access may constitute a violation, or violations of U.S. criminal laws, including the provisions of sections 641, 793, 794, 798, and 1924, Title 18, U.S.C., and the provisions of the Intelligence Identities Protection Act of 1982. You will not, without proper authorization, divulge the classified national security information disclosed to you, nor will you reveal to any individual your knowledge of the existence of such information. **THE RESPONSIBILITY TO SAFEGUARD THIS INFORMATION DOES NOT EXPIRE.**

Although you inadvertently gained information not intended for you, your signature below does not constitute an indoctrination or clearance for such classified information.

I,_____, hereby affirm that I have read and understand the instructions above for maintaining the security of classified national security information. I certify that I will never, without proper authority, divulge any properly classified national security information which I may have learned or which has been disclosed to me, nor will I reveal to any individual my knowledge of the existence of such information. I further certify that I will never attempt to gain access to such information by virtue of this inadvertent disclosure.

Printed Name and Signature:		
Subscribed to me this	day of	20

WITNESS Printed Name and Signature:

In accordance with DHS Instruction 121-01-011, the inadvertent disclosure of classified information to a person who is not authorized access to it requires the recipient of the information to sign an Inadvertent Disclosure Statement. If the person refuses to sign the Inadvertent Disclosure Statement, the information on this form must be read orally to the person, in the presence of a witness, and the form must be annotated to reflect the individual's refusal to sign.

Appendix G. Abbreviations and Acronyms

ASD	Administrative Security Division
C.F.R.	Code of Federal Regulations
CAPCO	Controlled Access Program Coordination Office
CBP	U.S. Customs and Border Protection
CCSO	Component Chief Security Officer
CDC	Classified Document Custodian
COMSEC	communications security
CSIRC	Computer Security Incident Response Center
CUSR	Central United States Registry
DCI Only	Director of Central Intelligence Only
DHS	Department of Homeland Security
DHS/CAP	DHS Classification Appeals Panel
DHS PALMS	DHS Performance and Learning Management System
DISCO	Defense Industrial Security Clearance Office
DNI Only	Director of National Intelligence Only
DOD	Department of Defense
DOS	Department of State
DSO	Designated Security Officer
DSS	Defense Security Service
E.O.	Executive Order
FAR	Federal Acquisition Regulation
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSO	Facility Security Officer
GAO	Government Accountability Office
GPO	Government Printing Office
GSA	General Services Administration
HSDN	Homeland Secure Data Network
IDS	intrusion detection system
IOD	Investigative Operations Division
ISCAP	Interagency Security Classification Appeals Panel
ISMS	Integrated Security Management System
ISOO	Information Security Oversight Office
IT	information technology
JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
LOU	Limited Official Use

MD	Management Directive
MFR	Memorandum for Record
MR	Manual Review
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NOFORN	Not Releasable to Foreign Nationals
OADR	Originating Agency's Determination Required
OCA	Original Classification Authority
OCC	Office of the Chief Counsel
OCSO	Office of the Chief Security Officer
OF	Optional Form
OI	Office of Intelligence
OPR	Office of Professional Responsibility
ORCON	Originator Controlled
OUO	Official Use Only
PEDs	Portable Electronic Devices
PIV	Personal Identity Verification
PROPIN	Caution – Proprietary Information Involved
PSD	Personnel Security Division
RD/FRD	Restricted Data/Formerly Restricted Data
REL	Releasable to
RELIDO	Release Determined by Foreign Disclosure Official
RFP	Request for Proposal
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SF	Standard Form
SLTPS	State, Local, Tribal, and Private Sector
SMD	Security Management Division
SSI	Sensitive Security Information
TSA	Transportation Security Administration
U.S.C.	United States Code
UL	Underwriters Laboratories