



Information and Administrative Security Program

PROTECTION OF CLASSIFIED INFORMATION

Office of Chief
Administrative Officer

June 2023

Version 1.2

Approval

 6/15/2023

Bradley Jewitt
Chief Administrative Officer

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

NOTE: *This Handbook establishes procedures, program responsibilities, minimum standards, and reporting protocols for the U.S. Department of Housing and Urban Development (HUD) Information and Administrative Security Program (IASP) for the protection of classified information, assignment of responsibilities and providing procedures for the designation, marking, protection, and the dissemination of classified information. The guidance herein was developed in accordance with Executive Order (EO) 13526: Classified National Security Information and Title 32 Code of Federal Regulations (CFR) Part 2001: Classified National Security Information. Combined, they form HUD's Information and Administrative Security Program (IASP), defining responsibilities and procedures for U.S. Department of Housing and Urban Development (HUD) and must be applied accordingly.*

REVISION: This revised Handbook supersedes *HUD Administrative Security Program*, dated 1991.

SUMMARY OF CHANGES:

Chapter 4. Provides guidance for safeguarding, storage, destruction, transmission, and transportation of classified information. Chapter 1, Section 5. Identifies security education and training requirements and processes for handling of security violations and compromise of classified information. Chapter 5, Section 5. Addresses information technology issues of which the security manager must be aware.

1. **SCOPE:** This Handbook applies to all U.S. Department of Housing and Urban Development (HUD) offices (hereinafter "HUD Offices"), including Headquarters, Regions, and Field Offices, and all other organizational entities within HUD, and does not alter existing authorities and responsibilities of the Director of National Intelligence (D/Ni) or of the heads of elements of the Intelligence Community (IC) pursuant to policies issued by the D/Ni. Sensitive Compartmented Information (SCI) shall be safeguarded in accordance with the policies and procedures issued by the D/Ni.
2. **PURPOSE:** This Handbook identifies and protects national security information with national-level policy issuances; promotes information sharing, facilitates judicious use of resources, and simplifies management through implementation of uniform and standardized processes; employs, maintains, and enforces standards for safeguarding, storing, destroying, transmitting, and transporting classified information; actively promotes and implements security education and training throughout HUD; and mitigates the adverse effects of unauthorized access to classified information by investigating and acting upon reports of security violations and compromises of classified information.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

TABLE OF CONTENTS

| | |
|--|-----------|
| Chapter 1: Overview | 6 |
| Acronyms..... | 6 |
| Authorities and References | 8 |
| Responsibilities..... | 8 |
| Supersession | 11 |
| Questions..... | 12 |
| CHAPTER 2: Classification Management..... | 13 |
| Original Classification | 13 |
| Derivative Classification..... | 15 |
| Classification Challenges..... | 17 |
| Raising the Classification Level | 18 |
| Declassification..... | 19 |
| Chapter 3: Access to Classified Information..... | 23 |
| Access | 23 |
| Visit Notifications..... | 25 |
| Emergency Notifications..... | 25 |
| Chapter 4: Safeguarding and Storage..... | 27 |
| Safeguarding..... | 27 |
| Certification Reciprocity | 32 |
| Closed Storage | 32 |
| CSPA..... | 36 |
| Open Storage | 36 |
| Accountability..... | 46 |
| Transmission and Transportation | 47 |
| Reproduction | 52 |
| Disposition and Destruction of Classified Material | 53 |
| Alternative Control Measures and Waivers | 54 |
| Chapter 5: Security Violations and Infractions..... | 55 |
| Reporting a Security Incident | 55 |
| Reportable Security Incidents..... | 55 |
| Security Inquiries | 56 |
| Formal Investigation | 58 |
| Incidents Involving Classified Information Within Information Technology (IT) Systems (Classified Spillage)..... | 59 |
| Security Violations and Infractions in Foreign Countries | 59 |
| Other Agency Security Violations and Infractions..... | 60 |
| Sanctions..... | 60 |
| Chapter 6: Classified FGI..... | 62 |
| General | 62 |
| Classification | 62 |
| Declassification..... | 62 |
| Access | 63 |
| Storage..... | 63 |

FOR OFFICIAL USE ONLY (FOUO)

| | |
|--|-----------|
| Transmission | 63 |
| Transfer | 63 |
| Accountability and Reproduction | 63 |
| Chapter 7: Marking | 65 |
| General | 65 |
| Originally Classified Documents | 65 |
| Derivatively Classified Documents | 66 |
| Working Papers | 69 |
| Transmittal Documents | 69 |
| Other Materials | 69 |
| Declassification Markings | 70 |
| Electronic Markings | 70 |
| Chapter 8: Security Education, Training, and Awareness (SETA) Program | 75 |
| General | 75 |
| Original Classification Authority Training | 75 |
| Derivative Classifier Training | 76 |
| Termination Briefings | 76 |
| Other Specialized Training | 76 |
| Documentation Requirements | 77 |
| Chapter 9: Security Compliance Review Program | 78 |
| General | 78 |
| Announcements and Conduct | 78 |
| Self-Inspection Programs | 79 |
| Chapter 10: Industrial Security Program | 80 |
| General | 80 |
| National Industrial Security Program Operating Manual (NISPOM) | 80 |
| Program Management | 80 |
| Chapter 11: Administrative Security Reporting Requirements | 85 |
| Reporting of Original Classification Authorities | 85 |
| Reporting of Security Compliance Review Activities | 85 |
| Fundamental Security Classification Guide Review | 85 |
| Classification Cost Reporting | 85 |
| Classification Activity Report (311 Reporting) | 85 |
| Chapter 12: Standard Forms | 86 |
| General | 86 |
| Availability | 86 |
| Standard Forms | 86 |
| APPENDIX A: Definitions | 91 |
| Appendix B: Forms | 99 |

FOR OFFICIAL USE ONLY (FOUO)

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

5 | Page

CHAPTER 1: OVERVIEW

ACRONYMS

| | |
|----------------|--|
| A/S | Assistant Secretary |
| CAO | Chief Administrative Officer |
| CAP | Classification Appeals Panel |
| CAPCO | Controlled Access Program Coordination Office |
| CCSO | Component Chief Security Officer |
| CNSSI | Committee on National Security Systems Instruction |
| CMP | Classification Management Program |
| COOP | Continuity of Operations |
| CNSSP | Committee on National Security Systems Policy |
| COMSEC | Communications Security |
| CFR | Code of Federal Regulations |
| CISO | Office of the Chief Security Officer |
| CSO | Component Security Officer |
| CSPA | Closed Storage Processing Area |
| CUSR | Central US Registry |
| CVS | Clearance Verification System |
| D/NI | Director of National Intelligence |
| D/S | Deputy Secretary |
| DCID | Director of Central Intelligence Directives |
| DCS | Defense Courier Service |
| DISCO | Defense Industrial Security Clearance Office |
| DoD | Department of Defense |
| DOJ | Department of Justice |
| DOS | Department of State |
| DRS | Declassification Review System |
| DSS | Defense Security Service |
| EO | Executive Order |
| FED-STD | Federal Standard |
| FDO | Foreign Disclosure Office |
| FGI | Foreign Government Information |
| FOIA | Freedom of Information Act |
| FRD | Formerly Restricted Data |
| FSO | Facility Security Officer |
| GAO | Government Accountability Office |
| GCA | Government Contracting Office |
| GPO | Government Printing Office |
| HSDN | Homeland Secure Data Network |
| HUD | U.S. Department of Housing and Urban Development |
| IC | Intelligence Community |
| ICD | Intelligence Community Directives |
| IDE | Intrusion Detection Equipment |

FOR OFFICIAL USE ONLY (FOUO)

| | |
|----------------|--|
| IDS | Intrusion Detection Alarm System |
| ISA | International Security Agreements |
| ISCAP | Interagency Security Classification Appeals Panel |
| IASP | Information and Administrative Security Program |
| ISSO | Information System Security Officer |
| MR | Manual Review |
| NARA | National Archives and Records Administration |
| NATO | North Atlantic Treaty Organization |
| NDA | Non-Disclosure Agreement |
| NISP | National Industrial Security Program |
| NOFORN | Not Releasable to Foreign Nationals |
| NSI | National Security Information |
| NSO | National Security Officer |
| NTISSI | National Telecommunications Information Systems Security Instruction |
| OADR | Originating Agency's Determination Required |
| OCA | Original Classification Authority |
| OCAO | Office of Chief Administrative Officer |
| OCHCO | Office of Chief Human Capital Officer |
| ODNI | Office of the Director of National Intelligence |
| OF | Optional Form |
| OGC | Office of the General Counsel |
| OIG | Office of Inspector General |
| OGC | Office of the General Counsel |
| OPM | Office of Personnel Management |
| OPR | Office of Professional Responsibility |
| ORCON | Originator Controlled |
| OSAF | Open Storage Area Facility |
| OSEP | Office of Security and Emergency Planning |
| OSL | Office Security Liaison |
| PED | Portable Electronic Devices |
| PROPIN | Caution—Proprietary Information Involved |
| PSO | Personnel Security Office |
| Pub. L. | Public law |
| RD | Restricted Data |
| REL | Releasable to |
| RELIDO | Release Determined by Foreign Disclosure Official |
| ROI | Reports of Investigation |
| SAO | Senior Agency Official |
| SAP | Special Access Program |
| SCG | Security Classification Guide |
| SCI | Sensitive Compartmented Information |
| SCIF | Sensitive Compartmented Information Facilities |
| SCR | Security Compliance Review |
| SLTPS | State, Local, Tribal, and Private Sector |
| SOP | Standard Operating Procedure |

FOR OFFICIAL USE ONLY (FOUO)

| | |
|------------|---------------------------|
| SSO | System Security Officer |
| UL | Underwriters Laboratories |
| URL | Uniform Resource Locator |
| USC | U.S. Code |

AUTHORITIES AND REFERENCES

- A. Pub. L. 96-456, *Classified Information Procedures Act* (October 15, 1980), as amended by Pub. L. 111-16 (May 7, 2009)
- B. Pub. L. 107-296, *Homeland Security Act of 2002*
- C. Pub. L. 80-235, *National Security Act of 1947* (July 26, 1947), as amended by Pub. L. 117-103 (March 5, 2022)
- D. EO 12829, *National Industrial Security Program* (January 6, 1993)
- E. EO 12968, *Access to Classified Information* (August 4, 1995)
- F. EO 13284, *Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security* (January 23, 2003)
- G. EO 13526, *Classified National Security Information* (December 29, 2009)
- H. EO 13286, *Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security* (February 28, 2003), as amended by The Interagency Security Committee and Security Standards (April 22, 2005)
- I. 32 CFR Part 2001, *Classified National Security Information*
- J. 32 CFR Part 2004, *National Industrial Security Program (NISP)*
- K. 49 CFR Part 1520, *Protection of Sensitive Security Information*
- L. 32 CFR Part 117, DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)* (February 2006), as amended via Change 2 (May 18, 2016)
- M. NTISSI 4004.1, *Routine Destruction and Emergency Protection of COMSEC Material* (January 10, 2008)
- N. FED-STD 809D, *Inspection, Modification, Neutralization and Repair of GSA Approved Containers and Vault Doors* (April 14, 2018)
- O. CNSSP 16, *National Policy for the Destruction of COMSEC Paper Material* (May 4, 2021)
- P. UL 634 Ed. 12-2009, *Standard for Safety Connectors and Switches For Use With Burglar-Alarm Systems*
- Q. FF-L-2740 Rev. B, *Federal Specification: Locks, Combination, Electromechanical* (June 15, 2011)
- R. FF-P-110J, *Federal Specification: Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)* (March 11, 1994), as amended by FF-P-110H (February 11, 1997)
- S. FF-S-2738A, *Federal Specification: Seals, Antipilferage* (March 30, 1999), as amended by FF-S-2738 (June 7, 1990)

RESPONSIBILITIES

- A. The D/S, HUD, has delegated authority to the CAO to serve as the SAO for HUD's COOP Program, managing access to and protecting HUD-classified programs and information, and maintaining

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

and operating classified systems.¹ To execute this responsibility, the CAO, pursuant to Section 5.4.(d) of [EO 13526](#), shall coordinate across HUD Offices to:

1. Direct and administer the Department's program under which information is classified, safeguarded, and declassified.
2. Coordinate the Department's classification management program and serve as the HUD point of contact on matters associated with the ISOO.
3. Promulgate and publish implementing directives as necessary for program implementation and ensure procedures are established and implemented to prevent unauthorized and unnecessary access to classified information.
4. Disseminate implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public.
5. Establish and maintain security education and training programs.
6. Establish and maintain a self-inspection and periodic review program to review and assess the management and safeguarding of classified information created and/or possessed by HUD Program Offices and reporting annually to the Director of the Information Security Oversight Office on HUD's self-inspection program.
7. Develop special contingency plans for the safeguarding of classified information.²
8. Ensure the performance contract or other system used to rate personnel performance, includes the management of classified information, as a critical element to be evaluated in the rating of:
 - a. Security Managers, security specialists, or other officials performing security functions involving the safeguarding of classified information; and
 - b. Other personnel whose duties involve the creation or handling of classified information.
9. Account for costs associated with the implementation of programs for the protection of classified information. Report such costs to the ISOO upon request.
10. Assign personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of [EO 12958](#), as amended, that pertains to classified information that was

¹ ACTION—Designation of Senior Agency Official for Continuity of Operations, Dated August 24, 2022

² Including, but not limited to, incidents that impact facilities and affect HUD's ability to maintain required security controls and measures to affect classified information.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

managed by an Office of HUD that no longer exists and for which there is no clear successor in function.

11. Report violations, take corrective measures, and assess appropriate sanctions as warranted, in accordance with [EO 12958](#), as amended.
12. Oversee HUD's participation in SAPs authorized under [EO 12958](#), as amended.
13. Establish procedures to prevent unnecessary access to classified information, including procedures that:
 - a. Require that a need for access to classified information is established before initiating administrative clearance procedures; and
 - b. Ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.
14. Establish a secure capability to receive information, allegations, and/or complaints regarding over-classification or incorrect classification within the Agency, and to provide guidance to personnel on proper classification (as needed).
15. Perform any other management duties as required by Chief, DMNS that the Secretary may designate.

B. A/S, Administration, is responsible for:

1. Ensuring that the standards cited in this Handbook are effectively implemented and that those persons whose duties significantly involve handling of classified information, are documented as part of their performance elements as well as are rated on their ability to successfully carry out such duties.
2. Certifying that sufficient resources are in place to implement and manage the ISP and the requirements of this Handbook.
3. Appointing a senior official within each office to serve as the OSL.

C. Director, Emergency Management, is responsible for:

1. Developing, facilitating, and completing projects that involve national security.
2. Serving as the primary advisor on all federal statutes, EOs and directives on National Security.
3. Assessing organizational needs to ensure that regulatory needs are addressed, and that policies, planning, and program investments comply with federal policies and HUD regulations.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

4. Assisting in resolving policy issues, by developing approaches and in completing various reports and analytical research, while also helping to build capacity within the agency to meet statutory and regulatory requirements.
- D. Office Security Liaison, is responsible for supporting the Deputy Chief on security issues and ensuring that security programs meet the mission requirements of the Department. The OSL shall:
1. Serving as the primary security contact for the Office on all matters relating to implementation and compliance with the provisions of this directive.
 2. Implementing, monitoring, and managing, and overseeing the provisions of this directive within his/her respective Office.
 3. Liaising between the Office, Office counterparts, OCAO national security staff, and other security officials both inside and outside of government.
 4. Participating in annual security education and training program.
- E. Supervisors and Managers, are responsible for:
1. Ensuring that they are aware of and comply with the applicable provisions of this Handbook, and promote and ensure compliance by employees.
 2. Participating in HUD's Security Training, and ensuring that any staff assigned to perform national security responsibilities and classified duties, participate in security education and awareness training as required.
- F. All Personnel, are responsible for:
1. Protecting classified information from unauthorized disclosure, including marking and safeguarding requirements for classified national security information.
 2. Being aware of and complying with the applicable provisions of this Handbook and reporting to appropriate officials, infractions and/or violations that affect the safeguarding of classified information.
 3. Participating in all required annual security training and complying with all requirements for recognizing, identifying, and safeguarding protected information for which they are granted access.
 4. Ensuring the protection from divulging any of the protected categories of information outlined in this Handbook without proper authority. Failure to do so may result in administrative or disciplinary action, civil penalty, or other enforcement or corrective action.

SUPERSESSION

This Handbook supersedes and cancels all prior National Security policy, including HUD *Handbook National Security Information 1750.1*.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

QUESTIONS

All questions or concerns regarding this Handbook must be submitted to the OCAO SSO via HUD.SSO@hud.gov.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CHAPTER 2: CLASSIFICATION MANAGEMENT

Effective administration of the HUD CMP requires consistent application of policy and procedure. The integrity of the classification system is dependent upon the knowledge and judgment of officials involved in oversight, implementation, and application of the safeguarding and classification process. The consequences of an undefined and inconsistent program are wasted resources, lack of public trust, and potential harm to the national security.

This Handbook prescribes the minimum standards for the protection of classified information. Offices may exceed the standards cited in this directive but may not lessen them. Where an Office chooses to exceed the standards as cited herein, sufficient justification must exist to warrant any increased standard(s).

ORIGINAL CLASSIFICATION

- A. Authority: An OCA is an official authorized, in writing, either by the President, by agency leaders, or other officials delegated by the President, to make an initial determination to classify information. EO 13526 Sec 1.3 describes who has classification authority. The authority to classify information originally may be exercised only by:

- The President and the Vice President;
- Agency leaders/officials designated by the President; and
- U.S. Government officials delegated this authority pursuant to Paragraph (c) of Section 1.3 of EO 13526.

Further, classification levels provide context of and support to proper safeguarding and handling of classified information.

1. Classification Levels: At the time of original classification, the OCA assigns a classification level. Except as otherwise provided by statute, no other terms are used to identify U.S. classified information. Further, these terms are not to be used or applied to unclassified information that do not meet the standards for classification in accordance with this Handbook and EO 13526. There are only three (3) authorized classification levels:
 - a. TOP SECRET - 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 - 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 - 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.

FOR OFFICIAL USE ONLY (FOUO)

2. Communicating Classification Decisions:
 - a. Classification decisions made are communicated through publication of an SCG, and are issued by an OCA.
 - b. SCGs identify the elements of information regarding a specific subject to be classified, and establish the level and duration of classification for each element.
 3. Classification Prohibitions: Information is not classified to:
 - a. Conceal violations of law, inefficiency, or administrative error;
 - b. Prevent embarrassment to a person, organization, or agency;
 - c. Restrain competition;
 - d. Prevent and/or delay the release of information not requiring protection in the interest of national security; or
 - e. Relate to basic scientific information not clearly related to national security.
 4. Classification by Compilation
 - a. A compilation of items of information that are individually unclassified, may be classified in certain circumstances if the compilation reveals an additional association or relationship that meets the standards and criteria for classification under [EO 13526, Section 1.4., Classification Categories](#).
 - b. Additional association or relationship is not otherwise evident or revealed in the individual items of information; and the information is classified by an OCA.
 - c. When the determination is made that classification by compilation is necessary, the OCA provides explicit instructions as to what elements of the compilation, when combined, constitute classification.
 - d. Information classified at a lower level, when compiled with other information classified at a lower level, may be classified at a higher level, under the conditions cited above.
 5. Classifying Equipment: The overall classification of a piece of equipment or physical object is based on the highest classification of integrated parts.
- B. Dissemination Controls: An OCA may further add one or more of the below dissemination controls:
1. NOFORN: 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, they may

FOR OFFICIAL USE ONLY (FOUO)

designate it to NOFORN to preclude sharing requests. OCAs must carefully consider the consequences of applying the NOFORN designation to information.

2. ORCON: The application of ORCON designation requires that further dissemination beyond 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 and must carefully consider the consequences of applying the ORCON designation to information.
5. REL: The application of REL, followed by the applicable CAPCO approved tri-graph or tetra-graph, indicates that information has been approved to be releasable to the countries or organizations listed. Where applicable, the designation of REL should be done in coordination with the appropriate FDO.
6. RELIDO: 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 FDO.
7. PROPIN: 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.

DERIVATIVE CLASSIFICATION

A. Derivative Classification Authority

1. DCA is tied to an individual or position that has an official need to derivatively classify.
2. Before being authorized to derivatively classify, individuals are identified, trained, and certified based on the following, established HUD standards:
 - a. Identification: The OSL will identify those individuals or positions that have a need to derivatively classify material and submit the names of those individuals to DMNS for review and approval.
 - b. Training: DMNS will advise and coordinate all related training. Each Derivative Classifier receives initial training to prevent over-classification, as well as refresher training at least once every two (2) years, in order to retain their derivative classification authority.
 - c. Certification: Before a Derivative Classifier is certified, they must complete the required training to demonstrate that they are aware of proper derivative classification procedures and markings.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- i. The OSL is responsible for gathering an individual's Certificates and submitting them to DMNS for review.
- ii. Certifications are valid for up to two (2) years throughout HUD. Should an individual transfer between Offices, they do not need to be recertified until the end of the two (2) year period.
- iii. Upon the expiration of a certification, an individual may not derivatively classify until they are recertified. A waiver, not to exceed sixty (60) days, may be granted by the Chief/Deputy Chief Disaster and NSO, through DMNS, and is dependent upon operational circumstances.
- iv. An individual may be required to take remedial training, including being recertified, and/or may have their DCA revoked by the CSO for failure to properly protect classified information resulting in a security infraction or violation.

B. Derivative Classification Applications

1. If an individual applying derivative classification markings believes the paraphrasing, restating, and/or summarizing of classified information has changed the level of or removed the basis for classification, they must consult the appropriate OCA for a classification decision.
2. When applying derivative classification markings:
 - a. Classification markings cited on the source or in a security classification guide are 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, position or personal identifier, is placed on the newly created material.
 - c. Markings are applied according to the requirements of EO 13526, 32 CFR Part 2001, and [ISOO Booklet: Marking Classified National Security Information, Revision 4](#) (January 2018). Implementation must be in accordance this Handbook.
 - d. Questions on classification markings, as the markings appear on the source or in a security classification guide, are referred to the originator. For challenges to classification refer to *Classification Challenges*.
 - e. If practical, where classified information constitutes a small portion of an otherwise unclassified document, the Derivative Classifier will use a classified addenda and/or prepare a product in unclassified form to allow for maximum dissemination.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

C. Records of Derivative Classification Actions

1. Persons performing derivative classification actions must maintain a record of each action taken. For derivatively classified documents, the record will include the total number of documents derivatively classified, delineated by classification level.
2. Records are maintained by fiscal year and submitted to Chief/Deputy Chief, DMNS as part of annual reporting requirements.
3. Records of classification actions are counted and reported by document (not by page).

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.

D. Dissemination of Other Agency Information

1. Classified information originating in a given agency may be disseminated to another agency and/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, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information.
 - a. In the case of classified information relating to intelligence sources, methods, and activities, the Director of National Intelligence determines when such prior authorization is required.

CLASSIFICATION CHALLENGES

In circumstances where authorized holders of classified information, who, in good faith, believe the classification status is improper, they are encouraged and expected to challenge the classification status. Classification challenges are presented to the Classifier of the information.

NOTE: Where necessary, assistance and/or anonymity in processing a classification challenge can be obtained by processing the challenge through the Chief/Deputy Chief, DMNS.

A. Processing Formal Classification Challenges

1. Formal challenges to classification must be submitted in writing and presented to the OCA having jurisdiction over the challenged information. For each type of challenge, the following applies:
 - a. Unclassified
 - i. Must take every precaution to ensure it remains unclassified.
 - b. Classified

FOR OFFICIAL USE ONLY (FOUO)

- i. Must be marked and safeguarded accordingly.
 2. All correspondence must sufficiently describe the information being challenged and briefly explain why the information is classified or why it is classified at a particular level.
 3. Challenges may be received from any authorized holder of the information, to include HUD employees, contractors, employees and contractors of other Federal Agencies, or State, local, tribal, and private sector partners.
 4. Individuals wishing to submit formal challenges to classification must provide written statement to the Deputy Chief, DMNS who will then forward the challenge to the OCA and/or convene a panel to review the challenge, and make a formal determination.
 - a. Individuals submitting a classification challenge will not be subject to retribution for bringing such actions. DMNS honors a challenger's request for anonymity and serves as the agent for the challenger in processing the challenge.
 - b. The OCA receiving the challenge provides a written response with a classification/declassification decision to the challenger within sixty (60) days of receipt.
 5. The individual submitting the challenge has a right to appeal the decision to the ISCAP established by [EO 13526, Section 5.3, Interagency Security Classification Appeals Panel](#).
 6. Challenged information will remain classified and is protected at its highest level of classification until a final classification determination is made by DMNS, the appropriate OCA, and/or the ISCAP.
- B. Informal Classification Challenges

The classification challenge provision does 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 will ensure 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 is maintained with a file copy of the document. The OCA making the decision is responsible for notifying holders of the change in classification.

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 OCA and have cognizance over the information. Information may be raised to a higher level³ of classification, only if holders of the information can be notified of the change

³ HUD does not currently retain the authority to raise the classification level, and can only do so if directed by an OCA.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

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.

DECLASSIFICATION

Information shall remain classified as long as it is in the best interest of national security to keep it protected, and continued classification is in accordance with the requirements of the [EO 13526](#).

- A. If an employee has reason to believe that the public interest in disclosure of information outweighs the need for continued classification, they will refer the matter to the appropriate OCA or the HUD SAO for an assessment and determination on whether declassification is appropriate.
- B. None of the provisions cited herein apply to information classified in accordance with [10 CFR Part 1045, Nuclear Classification and Declassification of Restricted Data \(RD\) and Formerly Restricted Data \(FRD\)](#), or NATO classified information.
- C. Automatic Declassification at Twenty-Five (25) Years

- 1. Automatic Declassification of Permanent Historical Records

[EO 13526, Section 3.3, Automatic Declassification](#), mandates that information contained within permanently valuable historical records (as defined by [USC Title 44, Disposal of Records](#)) be automatically declassified twenty-five (25) years from the date of origin of the document. All classified records are automatically declassified on December 31 of the year that is twenty-five (25) years from the date of origin, except where such information has been exempted from automatic declassification at twenty-five (25) years.

- 2. 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 under this section, 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. For the purposes of automatic declassification, integrated file blocks contain only records dated within ten years of 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 HUD Senior Agency Official may delay automatic declassification for up to five (5) 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.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- c. By notification to the Director, ISOO, the Secretary or HUD Senior Agency Official 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.

D. Mandatory Review for Declassification

1. Any individual, except those identified in 5. below, may request a review for declassification of information classified under EO 13526, or its predecessor orders. Such requests must be sent to HUD's Chief Government Information Management Officer within the Office of Privacy and Freedom of Information Act.
2. Declassification does not apply to any request for a review made to an element of the intelligence community that is requested by a person other than a U.S. citizen, legal permanent resident, foreign government entity, or representative thereof.
3. Documents required to be submitted as part of a prepublication review or other administrative process pursuant to an approved non-disclosure agreement are not covered by this section.
4. 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.
5. Responsibilities

a. Chief Government Information Management Officer

- i. Serves as the central processing point for all mandatory review requests concerning HUD information;
- ii. Forwards mandatory review requests to the applicable HUD Office(s) having primary jurisdiction over the requested information and to Senior Agency for Intelligence for final determination on the protection/redaction of any classified information in collaboration with Office of General Counsel within thirty (30) days of receipt; and
- iii. Provides the requester with an acknowledgment of receipt of the request within five (5) calendar days.

b. Program Offices

- i. Promptly process the request within seven (7) calendar days unless otherwise requested or expedition is required;
- ii. Perform a line-by-line review; and

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- iii. Determine whether it is necessary to declassify the information if it no longer meets the standards for classification established by EO 13526 and this Handbook. If so, the declassified information will be released to the requester, unless withholding is appropriate under applicable law.

EXAMPLE: Freedom of Information Act or the Privacy Act of 1974.

6. Processing Mandatory Review Requests

- a. The request describes the document or material with enough specificity to allow it to be located by the Office with a reasonable amount of effort. Requests for broad types of information, entire file series of records, or similar non-specific requests are denied. When the description of the information in the request is deficient, the Office solicits 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 Office provides the requester, through the Chief Government Information Management Officer, with written notification of the reasons why no action is being taken and of the requester's right to appeal.
- b. Requests for review of information that has been subjected to a declassification review request within the preceding two years is not required to be processed. The Chief Government Information Management Officer notifies the requester of such denial.
- c. Requests for information exempted from search or review under Sections 105C, 105D, or 701 of the National Security Act of 1947 (50 U.S.C. 432, 432a, and 431), are not processed. The Chief Government Information Management Officer notifies the requester of such denial.
- d. If documents or material being reviewed for declassification under this Section contain information that has been originally classified by another government agency, the reviewer will notify the Chief Government Information Management Officer, who will then refer the matter to the originating agency.
- e. Unless the association of that organization with the requested information is itself classified, the Chief Government Information Management Officer will notify the requester of the referral.
- f. If the existence of the information is classified, the HUD Office should not confirm or deny the existence, or nonexistence, of requested information.
- g. The Chief Government Information Management Officer will maintain a record of all mandatory review actions for reporting, in accordance with applicable Federal requirements and provide an annual report to the SAO.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

7. Processing Appeals

The mandatory DRS provides for administrative appeals in cases where the review results in the information remaining classified. If this occurs:

- a. The Requester will be notified of the results of the review and of their right to appeal the denial of declassification. To address such appeals, the Chief Government Information Management Officer will refer the appeal to the SAO who in turn convenes a CAP. At a minimum, the CAP will consist of:

- i. Representatives from the Chief Government Information Management Officer, DMNS, the Office of the General Counsel; and
- ii. A representative from the Office having jurisdiction over the information.

Within sixty (60) days, the CAP will either, make a classification determination, or respond to the requester with a timeframe for making a determination.

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

E. FOIA and Privacy Act Requests

1. If a requester submits a request under both the Declassification provisions cited herein, and the Freedom of Information Act, the requester will be advised to elect one (1) process or the other. If the requester fails to elect either, the request will be treated as a FOIA request.
2. Upon receipt of a request for classified information under the Freedom of Information Act or the Privacy Act of 1974, the receiving office processes the request in accordance with the provisions of those Acts.

F. Downgrading

1. 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. The principal purpose of downgrading is to conserve security resources by avoiding protection of information at too high a level. Information may be downgraded by any official authorized to originally classify the information.
2. Existing documents that identify a specific date or event at which the information may be downgraded, are automatically downgraded upon occurrence of that date or event, unless the documents have been reviewed and the classification status has been changed by an OCA.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CHAPTER 3: ACCESS TO CLASSIFIED INFORMATION

ACCESS

- A. Access to classified information is limited to persons whose official duties require knowledge or possession of the information. No one has a right to have access to classified information solely by virtue of office, rank, or position. Three (3) criteria are required prior to granting access:
 - 1. Security Clearance: The intended recipient must possess a valid and appropriate security clearance equal to or higher than the level of classified information to which access will be granted.
 - 2. Non-Disclosure Agreement: The intended recipient must have executed an appropriate NDA.
 - 3. Need-to-Know: The intended recipient must have a valid need-to-know the information to perform a lawful and authorized governmental function.
- B. 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 A. of this Section have been met.
 - 1. Judicial: HUD OGC is consulted whenever a litigation request or demand is made upon HUD personnel for official HUD information or for testimony concerning such information. The person upon whom the request or demand was made, immediately notifies the Director, Emergency Management. Classified information is handled per the Classified Information Procedures Act (PL 96-456).
 - 2. Congress: Access to classified information or material by Congress, its committees, members, and staff representatives is coordinated through HUD, OCAO. Any HUD employee testifying before a Congressional committee in executive session, in relation to a classified matter, first obtains the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of information that may be discussed.
 - 3. SLTPS Officials: Access to classified information by SLTPS officials is consistent with the standards and requirements for access by executive branch personnel, as cited in EO 13549 and its implementing directive.
 - 4. GPO: Documents and material of all classifications may be processed by the GPO, which protects the information per the guidelines outlined in EO 13526.
 - 5. Representatives of GAO: Representatives of the GAO may be granted access to classified information when such information is relevant to the performance of the statutory

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

responsibilities of that office. Certifications of security clearances, and the basis thereof, is accomplished pursuant to arrangements between GAO and HUD Component concerned.

6. Historical Researchers: Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that a HUD and OCAO, with classification jurisdiction over the information, accomplishes the following:
 - a. 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 requester has been found to be trustworthy based on such investigation as determined by OCAO;
 - b. Limits such access to specific categories of information over which HUD Component has classification jurisdiction, and to any other category of information for which the researcher obtains the written consent of a HUD Component, or non-HUD Department or Agency that has classification jurisdiction over information contained in or revealed by the document, within the scope of the proposed historical researched;
 - c. Maintains custody of the classified material at a HUD installation or activity or authorizes access to documents in the custody of the NARA; and
 - d. Obtains the researcher's agreement to safeguard the information and to submit any notes and manuscripts for review by HUD Components or non-HUD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein. This agreement is included in a non-disclosure agreement, which is executed by the researcher as a condition of access.
 - i. Issues an authorization for access valid for not more than two (2) years from the date of issuance.
7. Former Political Appointees: Former political appointees may be authorized access to classified information they originally classified when in their position provided that a HUD Appointee, with current classification jurisdiction over the information, accomplishes the following:
 - a. 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 by certifying that the requester has been determined to be trustworthy based on such investigation as determined by OCAO;
 - b. Limits access to specific categories of information over which HUD has classification jurisdiction and to any other category of information for which the former appointee obtains the written consent of a non-HUD department or agency that has classification jurisdiction

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

over information contained in or revealed by documents within the scope of the proposed access;

- c. Retains custody of the classified material at a HUD installation or activity, or authorizes access to documents in the custody of the National Archives and Records Administrations; and
- d. Obtains the former presidential appointee's agreement, through the execution of a non-disclosure agreement, to safeguard the information and to submit any notes and manuscripts for review by HUD or non-HUD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein.

VISIT NOTIFICATIONS

Visits involving access to, or disclosure of, classified information shall include verification of the identity, personnel security clearance, access, and need-to-know for all visitors. Visits by officials such as members of Congress are coordinated through OCAO. Visit requests (security clearance verification) are submitted by the Security Office of the parent organization to OCAO SSO or PSO. Where access to an automated security clearance verification system is available, such as OPM's CVS, security clearances of visitors may be verified through the system in lieu of the transmission of hard copy visit requests. Visit requests hand-carried by a visitor are not honored or accepted.

EMERGENCY NOTIFICATIONS

In an emergency, and when necessary to respond to an imminent threat to life or in defense of the homeland, Director, Emergency Management may authorize disclosure of classified information to an otherwise unauthorized individual or individuals. Under these conditions, he/she may:

- A. Limit 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. Transmit the classified information via approved Federal Government channels by the most secure and expeditious method possible, or by other means deemed necessary when time is of the essence.
- C. Provide instructions about what specific information is classified and how it should be safeguarded. Physical custody of classified information remains with an authorized Federal Government entity in all but the most extraordinary and unique of circumstances.
- D. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement. In emergencies requiring immediate verbal release of information, the signed nondisclosure agreement memorializing the briefing may be received after the emergency abates.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

E. Within seventy-two (72) hours of the disclosure of classified information, or the earliest opportunity that the emergency permits but no later than seven (7) days after the release, the disclosing authority notifies the SSO and the originating Agency of the information. The notification must include:

1. A description of the disclosed information;
2. To whom the information was disclosed;
3. How the information was disclosed;
4. Reason for the emergency released;
5. How the Information was safeguarded; and
6. A description of the briefing provided and a copy of the signed NDA.

Upon completion, a copy of the NDA is forwarded with the notification to the SSO and originating Agency of the information.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CHAPTER 4: SAFEGUARDING AND STORAGE

SAFEGUARDING

- A. **Personnel:** Personnel who have been granted access to classified information are responsible for protecting the information in their possession or control, and ensuring proper precautions are taken to prevent unauthorized access. This includes ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.
- B. **Classified information:** Classified information is always protected either by storage in an approved container or facility or having it under the personal observation and control of an authorized individual.
- C. **No Comment Policy:** The protection of classified information is normally accomplished through security measures designed to prevent unauthorized disclosure. However, there are occasions when classified information or information that appears to be classified is published without authorization in the public domain, e.g., through newspapers, magazines, books, the internet, and television. In such cases, commenting on classified information that is in the public domain, or attempting to prevent its further dissemination, could result in greater damage to the national security than would occur if no comments were made about the information. Any questions raised about the accuracy, classification, or technical merit of such information should be responded to in a “No Comment” manner and/or referred to the Office of Public Affairs.
- E. **Care During Working Hours:** Items containing classified information, such as preliminary drafts, carbon sheets, worksheets, and printer ribbons, electronic media, and other items, are either destroyed immediately after the items have served the purpose intended or protected as required for the level of classified information the items contain. Any media containing classified information, in any form, is appropriately secured when unattended.
- F. **Combinations: Combinations and Computer and Information System Passwords.** Passwords shall be protected in the same manner as the highest level of classified information that the computer or system is certified and accredited to process. Passwords shall be changed on a frequency determined to be sufficient to meet the level of risk assessed by the System Administrator.
- G. **Cover Sheets:** Classified information removed from storage is kept under constant surveillance by authorized personnel. Standard Forms (SF) 703, 704, and 705, classified document cover sheets, are placed on classified documents when not in secure storage containers.
- H. **Classification Labels:** Electronic media and other media that contain classified information or information pending classification shall be labeled with SFs 706 (Top Secret), 707 (Secret), 708 (Confidential), 709 (Classified, pending classification), or 712 (SCI). In a mixed environment in which classified and unclassified information is being processed or stored, electronic media or other media

FOR OFFICIAL USE ONLY (FOUO)

dedicated for unclassified information shall be labeled with SF 710 to aid in distinguishing among those media that contain either classified or unclassified information. The SFs are affixed to the medium containing classified or unclassified information in a manner that would not adversely affect operation of equipment in which the medium is used. SFs may not be affixed to Communications Security (COMSEC) equipment to ensure the equipment remains tamper evident.

- I. Security Container Check Sheet: Use of the SF 702, Security Container Check Sheet, is mandatory to record the opening, closing, and checks of all vaults, open storage areas, and security containers that store classified information.
- J. Activity Security Checklist: Activities that process or store classified information establish and implement a system of security checks at the close of each working day to ensure that the area is secure and classified information has been properly stored. SF 701, Activity Security Checklist, is used to record such checks.
- K. Emergency Planning
 - 1. To minimize the risk of compromise, plans are developed for protecting, removing, or destroying classified information in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. The level of detail and amount of testing and rehearsal of these plans should be determined by an assessment of the risk of hostile action, natural disaster or terrorist activity that might place the information in jeopardy. These plans are reviewed for currency at least once a year.
 - 2. Planning for the emergency protection (including emergency destruction under no-notice conditions) of classified COMSEC material is developed per the requirements of the CNSSI number 4004.1, *Destruction and Emergency Protection Procedures for COMSEC and Classified Material*. When preparing emergency plans, consider reducing classified material on hand by destroying unneeded material, retiring unneeded material, or transferring unneeded material to automated information systems media.
- L. Telephone Conversations: Classified information is not discussed telephonically except over approved COMSEC equipment.
- M. Removal of Classified Storage Equipment: Storage containers used to store classified information are inspected by properly cleared personnel from SSO or COMSEC officer prior to removal from protected areas, or before unauthorized persons are allowed access to the containers. The inspections ensure that no classified information remains in the container.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

N. Residential Storage

1. ODMNS may authorize the storage of classified information in private residences. Requests for in-residence storage of classified information is submitted, with justification, through OCAO.
2. When residential storage is approved, a GSA-approved security container authorized for the storage of classified material must be utilized. Closed storage requirements outlined in Chapter 4 of this Policy must be implemented and followed in the space which contains the GSA-approved container. Written procedures are developed to provide for appropriate protection of the information, to include a record of the information that is authorized for residential storage. These procedures are coordinated through OCAO.

O. Classified Meetings and Conferences: Meetings and conferences that involve classified information present special vulnerabilities for unauthorized disclosure. Heads of OCAO, or their designees, establish specific requirements for protecting classified information at conferences, seminars, exhibits, symposia, conventions, training courses, or other such gatherings where classified information is present. For in-house gatherings and other impromptu meetings, see P. below. At a minimum, the following applies:

1. The meeting serves a specific U.S. Government purpose;
2. The use of other appropriate channels for dissemination of classified information or material is insufficient;
3. The meeting location is in the spaces of, and under the security control of a U.S. Government Agency, or a U.S. contractor with an appropriate facility security clearance; and
4. Meetings are not held in commercial spaces (e.g., hotel conference facilities) without prior approval and coordination SSO. In such instances the requester documents and submits a request to SSO, that includes the following:
 - a. affirmation that there is no U.S. Government or cleared contractor facility available at which classified sessions can be held;
 - b. That the information to be discussed cannot be declassified or sanitized to an unclassified level and still retain its value to the intended audience; and
 - c. The criticality or urgency that requires the information be presented at an unsecured location. Such requests are submitted as early in the meeting planning stage as possible.
5. Adequate security procedures are developed and implemented to minimize risk to the classified information involved.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

6. Classified sessions are segregated from unclassified sessions whenever possible.
 7. Access to the meeting or conference, or specific sessions thereof, at which classified information is discussed or disseminated, is limited to persons who possess an appropriate security clearance and need-to-know.
 8. Valid government-issued identification is used to verify the identity of attendees.
 9. Announcement of the classified meeting is limited to a general description of topics expected 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 HUD Component 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 U.S. Government purpose for the meeting and accommodations are made to ensure materials are properly secured and transported.
 10. HUD Component sponsoring the meeting appoints a SSO official to serve as the meeting.
 11. Other U.S. Government organizations or cleared HUD contractors with appropriate facility security clearances, may assist with implementing security requirements under the direction of the appointed SSO.
- P. Internal classified gatherings or other impromptu meetings: For in-house gatherings and other impromptu meetings where classified information is discussed, it is incumbent upon the host or sponsor of the meeting to ensure appropriate security measures are in place. Those measures include:
1. The meeting is held either in the spaces of, and under ODMNS control.
 2. Ensuring that all electronic equipment not authorized for the processing of classified information is removed from the room.
 3. Conducting a sound attenuation test to ensure normal conversational tone from inside the room cannot be heard intelligibly from outside the room (paying particular attention to vents, ducts, and other openings). If public address or other amplification systems are used, conduct the test with these systems on and off.
 4. Assigning and posting cleared host office personnel at exterior doors and hallways to keep the room's perimeter under surveillance and prevent passers-by from stopping and listening.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

5. Controlling access to the room. Use an attendee roster if applicable, and have sufficient backup host office personnel available, as needed.
 6. Verifying the identity of each participant via U.S. Government photo-identification or equivalent documentation.
 7. Ensuring the security clearances of attendees are at least equal to the level of classified information to be disclosed.
 8. Prohibiting those without proper authorization and clearance from attending classified portions of the meeting.
 9. Notifying each attendee and presenter of:
 - a. The highest level of classified information to be presented/discussed and when multiple presentations are given, the specific classification (or unclassified status) of each presentation;
 - b. Limits on the number of room entrances and the access control before or during the meeting to prevent access by unauthorized persons; and
 - c. Limitations associated with classified portions of the meeting, e.g., prohibitions against photographing, note-taking, audio/video recording, using two-way radios, cellular phones, or other transmitting devices.
 10. Ensuring security protection for the room is maintained during breaks.
 11. Complying with all security safeguards for classified information.
 12. After the meeting, inspecting the room to ensure no classified materials have been left behind.
 13. If applicable, and attendees have valid courier authorization cards or letters, ensuring sufficient supplies are available to properly package classified materials for local attendees to hand-carry back to their office.
- Q. U.S. Classified Information Located in Foreign Countries: Except for classified information that has been authorized for release to a foreign government, U.S. classified material may be retained in foreign countries only when necessary to satisfy specific U.S. Government requirements. The Director, Emergency Management prescribes requirements for the protection of this information, with particular attention to ensuring proper enforcement of controls or release of classified information to foreign entities. Classified material in foreign countries is stored:

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

1. Computer

- a. At a U.S. military installation, or a location where the United States enjoys extra territorial status, such as an embassy or consulate.
- b. At a U.S. Government entity located in a building used exclusively by U.S. Government tenants, provided the building is under twenty-four (24)-hour control by U.S. Government personnel.
- c. At 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. personnel have access.

R. Computer Equipment and Removable Storage Media: OCAO' COMSEC Officer has a variety of non-COMSEC-approved equipment used to process classified information. It includes copiers, facsimile machines, computer equipment and peripherals, word processing systems, and others. Components identify those features, parts, or functions of equipment used to process classified information that may retain all or part of the information. Component security procedures prescribe the appropriate safeguards to:

- 1. Prevent unauthorized access to the equipment and/or information.
- 2. 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.
- 3. At a U.S. Government entity located in a building used exclusively by U.S. Government tenants, provided the building is under twenty-four (24)-hour control by U.S. Government personnel.
- 4. Ensure that appropriately cleared and technically knowledgeable personnel inspect equipment before the equipment is removed from protected areas.

CERTIFICATION RECIPROCITY

If a facility is authorized, approved, certified, or accredited for classified use, then all Components desiring to conduct classified work in the designated space(s) at the same security level, should accept the authorization, approval, certification, or accreditation without change, enhancements, or upgrades provided that no waiver, exception, or deviation has been issued or approved.

CLOSED STORAGE

- A. Classified information is secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this Policy represent acceptable security standards. Weapons

FOR OFFICIAL USE ONLY (FOUO)

or sensitive items such as funds, jewels, precious metals, or drugs are not stored in the same container used to safeguard classified information. Security requirements for SCIFs are established by the Director of National Intelligence through various ICDs. Current holdings of classified material are reduced to the minimum required for mission accomplishment.

- B. Classified information is protected at all times either by storage in an approved container or facility or having it under the personal observation and control of an authorized individual Standards for Storage Equipment. Consult GSA supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information.
- C. New purchases of combination locks for GSA-approved security containers, vault doors and secure rooms conform to Federal Specification FF-L-2740. Existing non-FF-L-2740 mechanical combination locks are not repaired. If these locks should fail, the locks are replaced with locks meeting the FF-L-2740 standard.
- D. Maintenance performed on GSA-approved containers is in accordance with Federal Standard 809. When repairs to a GSA-approved container affect its original integrity, the GSA-approved label is removed, and the container is no longer authorized for the storage of classified information.
- E. Storage of Classified Information: Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked security container, vault, room, or area, as follows:
 - 1. Top Secret information is stored by one of the following methods:
 - a. A GSA-approved security container equipped with a lock meeting Federal Specification FF-L-2740 with one of the following supplemental controls:
 - i. Inspection of the container every two hours by an employee cleared at least to the Top-Secret level;
 - ii. An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation. Acceptability of IDE: All IDE is subject to approval by OCAO.
 - iii. Security-In-Depth, as determined by the SSO.
 - b. In a vault or GSA-approved modular vault meeting the requirements of Federal Standard 832, "Construction Methods and Materials for Vaults."
 - c. In an open storage area (secure room) accredited by ODMNS SSO and equipped with an IDS with the personnel responding to an alarm within the required time (15 or 5 minutes).

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

Personnel should respond 15 minutes of the alarm annunciation if the area has been determined to have security-in-depth by SSO, or within 5 minutes of alarm annunciation if it has not.

2. Secret information is 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 built to Federal Standard 832 without supplemental controls; or, in an open storage area accredited by OCAO SSO and equipped with an IDS with the personnel responding to an alarm within thirty (30) minutes of the alarm annunciation if the area has been determined to have security-in-depth by the SSO, or with an employee cleared to at least the Secret level inspecting the open storage area once every four (4) hours if it has not.
3. Confidential information is stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.
 - a. Open Storage: Approval of open storage is considered when the volume of materials or operational necessity of the mission dictates. OCAO SSO authorizes approval, in writing, for a space or office to be designated for the open storage of classified information. Open storage areas must be constructed to meet the following minimum standards:
 - i. Construction: The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in a manner as to provide visual evidence of unauthorized penetration.
 - ii. Doors: Doors shall be constructed of wood, metal, or other solid material. Entrance doors shall be secured with a built-in GSA-approved three-position combination lock. When special circumstances exist, the agency head may authorize other locks on entrance doors for Secret and Confidential storage. Doors other than those secured with the aforementioned locks shall be secured from the inside with either deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar which extends across the width of the door, or by other means approved by the agency head.
 - iii. Vents, Ducts, and Miscellaneous Openings: All vents, ducts, and similar openings in excess of ninety-six (96) square inches (and over six (6) inches in its smallest dimension) that enter or pass through an open storage area shall be protected with either bars, expanded metal grill, commercial metal sound baffles, or an intrusion detection system.
 - iv. Windows: All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings. Windows within eighteen (18) feet of the ground will be constructed from or covered with materials that provide protection from forced entry. The protection provided

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

to the windows needs to be no stronger than the strength of the contiguous walls. Open storage areas which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by the motion detection sensors within the area).

- b. Open Equipment Designations: There is no external mark revealing the level of classified information authorized to be or stored in, a given container or vault, or to the priority assigned to the container for emergency evacuation and destruction. This does not preclude placing a mark or symbol, (e.g., a barcode) on the container for other purposes (e.g., identification and/or inventory purposes).
- c. Combinations to Containers and Vaults: Only persons having an appropriate security clearance and need-to-know shall have access to combinations to security containers, vaults, and secure rooms used for the storage of classified information.
 - i. Combination of Container, Vault, or Secure Room: Used for the storage of classified information is treated as information having a classification equal to the highest category of the classified information stored therein. Any written record of the combination is marked with the appropriate classification level. The Standard Form 700 (SF 700), Security Container Information, is used for this purpose.
 - ii. GSA-approved field safes and special purpose one- and two-drawer, light-weight security containers, approved by the GSA, are used primarily for storage of classified information in the field. Such containers are securely fastened to a permanent structure or under sufficient surveillance to prevent theft.
 - iii. Combinations are changed:
 - a. When placed in use;
 - b. Whenever an individual knowing 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 subject to possible compromise;
 - d. When taken out of service. Built-in combination locks are then reset to the standard combination 50-25-50; combination padlocks are reset to the standard combination 10-20-30;
 - e. Every two years, if none of the above conditions have been applied.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CSPA

A CSPA is established when a sponsored organization has a requirement to process classified information using an approved HSDN closed storage configuration.

OPEN STORAGE

Any storage of classified national security information outside of approved containers is considered Open Storage, to include classified information that is resident on information systems media and outside of an approved storage container, regardless of whether or not that media is in use (i.e., unattended operations). Open Storage of classified cryptographic material and equipment must be done within an approved COMSEC facility, vault, or secure room when authorized personnel are not present. Construction and accreditation of a collateral-level, open-storage facility is considered only when the volume or bulk of classified material, or the functions associated with processing the classified material, make the use of GSA-approved security containers impractical.

- a. Existing Approvals: Open Storage areas that were approved before the publication of this Handbook need not have the areas re-certified unless a change has been made that affects the structure and measures in place at the time of the original approval. Open Storage for formerly approved areas is based on:
 1. Operational Justification: Open Storage areas are only approved for operational reasons, not for convenience. Where requested to satisfy the installation of a classified information system, unless otherwise justified and approved, the authorization is limited to the system only. All documents and removable media still require closed storage in an appropriate security container.
 2. Compliance with construction standards cited in this Policy.
 3. Completion of an SOP for operating the area. The Director, Emergency Management shall approve any SOP(s) before their implementation.
 4. Receipt of a Facility Accreditation Memorandum signed by the Director, Emergency Management.
- b. New Approvals: Open Storage areas that have not yet been approved, are required to obtain approval from the SSO, who has approval authority for the collateral open storage areas of HUD facilities. Upon approval of an area for open storage of collateral classified information, SSO issues a memorandum to the requesting Component, citing the specific location, building, room number, etc.; the level of classified information authorized for open storage; any restrictions; and any other information deemed appropriate. A copy of the approval memorandum, Open Storage Survey Checklist, and SOP are maintained by the approving authority and within the approved open storage area.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

c. Level of Storage

1. Top Secret: An open storage area for Top Secret material meets the construction standards and IDS requirements cited in Section 5. Arrival on-scene to unannounced alarm activations is within fifteen (15) minutes from the time the alarm is received at the monitoring station.
2. Secret: An open storage area for Secret material meets the construction standards cited in Section 5. Also, an IDS is installed that meets the standards cited in 5. Arrival on-scene to unannounced alarm activations is within thirty (30) minutes from the time the alarm is received at the monitoring station.
3. Confidential: Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.
4. PEDs: PEDs not introduced into an open storage area. Restrictions on the introduction of PEDs into open storage areas are prominently posted and included in the SOP. Exceptions are made only with written approval from the Designated Approval Authority in consultation with the cognizant Information Systems Security Manager and SSO. Approvals are considered only when the risks associated with the use of such equipment are clearly identified and sufficiently mitigate.

d. General Construction Requirements: These criteria and standards apply to all new construction, reconstruction, alterations, modifications, and repairs of existing areas. These criteria and standards are also used in evaluating existing areas.

1. All vents, ducts, and similar openings more than ninety-six (96) square inches (eleven (11)" diameter for circular ducts) that enter an OSAF are protected with either bars, or grills, or commercial metal duct sound baffles that meet the appropriate sound attenuation class. If one dimension of the duct measures less than six inches, or the duct is less than ninety-six (96) square inches, bars are not required; however, all ducts are treated to provide sufficient sound attenuation. If bars are used, the bars are a minimum ½ inch diameter steel welded vertically and horizontally six (6) inches on center; if grills are used, the grills are a minimum of thirteen (13)-gauge expanded steel; if commercial sound baffles are used, the baffles or wave forms are permanently installed metal and no farther apart than six (6) inches in one dimension. A deviation of ½ inch in vertical and/or horizontal spacing is permissible. An access port to allow visual inspection of the protection in the vent or duct may be installed inside the secure perimeter of the OSAF. If the inspection port is installed outside the perimeter of the OSAF, it is locked.
2. Doors: Are constructed substantially of wood or metal. When doors are used in pairs or a gap exposes the latching mechanism, an astragal (overlapping molding) is installed where the doors meet, or exposure occurs. It is preferred that hinges be on the secure side of the door. Hinge

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

pins that are exposed to the outer perimeter of the area are pinned, brazed, or spot-welded to preclude removal. All doors meet the following criteria:

- a. Solid core wood, minimum 1 ¾" inch thick, natural wood veneer, installed in welded steel frame assembly mounted to fourteen (14)-gauge metal studs. Knock down [collapsible jam and header] frame or aluminum frame is not acceptable.
 - b. Doors and frames meet or exceed an STC-45 equivalent rating in processing areas. Doors and frames meet or exceed an STC-50 equivalent rating in areas where there will be amplified sound. Doors have adjustable acoustical gasket around the door with an automatic threshold seal installed in these instances.
 - c. Doors with windows, louvers, baffle plates, or similar openings are only authorized to be used in areas with no processing or discussion. These items are secured with 13-gauge expanded metal securely fastened on the inside. If visual access is a factor, any windows are covered.
 - d. Doors are equipped with an industrial Grade 1 automatic door closer.
 - e. For new construction or renovation, entrance doors are secured with a GSA-approved, built-in combination lock meeting Federal Specification FF-L-2740. Other high security locks may be used on a case-by-case basis with the approval from Director, Emergency Management. Other doors are secured from the inside with a panic bolt (which can be actuated by an alarmed panic bar); a deadbolt; a rigid wood or metal bar (that precludes "springing"), which extend across the width of the door and is held in position by solid clamps, preferably on the door casing; or by other means approved by Director, Emergency Management consistent with relevant fire and safety codes.
 - f. Routine entrance doors are additionally equipped with a supplemental access control device (e.g., key lock, leverset, card reader, cipher lock, etc.,) to control access into the area during working hours. Supplemental access control devices are for access control purposes only and do not provide sufficient security for an unattended open storage area.
 - g. All door hardware meets Grade 1 standards.
 - h. All key locks meet UL 437 standards.
3. Windows: Every effort should be made to construct open storage areas without windows. But where the presence of windows is unavoidable, windows are covered by opaque window film, or by blinds turned to no more than a forty-five (45)-degree angle, permanently fastened at top and bottom, and not adjustable by the user ability to open the window is eliminated by either permanently sealing it or installing a locking mechanism on the inside. Windows that open and are less than eighteen (18) feet from grade or adjacent roofs, less than fourteen (14) feet from other structures, trees, or horizontal openings, or less than three (3) feet from openings on the same wall that are not part of the open storage space require one of the following:

FOR OFFICIAL USE ONLY (FOUO)

- a. Vertical round iron or steel bars, a minimum of ½" diameter spaced six (6)" on center. The bars may be mortised into the masonry, built into the frame, or equipped with horizontal crossbars for added strength and support.
- b. Vertical flat iron or steel bars, a minimum of 1 ½" x ⅜" spaced six (6)" on center. The bars may be mortised into the masonry, built into the frame, or equipped with horizontal crossbars for added strength and support.
- c. All fasteners are welded or specially manufactured to prevent removal.

4. Walls

- a. Walls, true floor, and true ceiling are permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, including above the false ceiling and below a raised floor, is done in such a manner as to provide visual evidence of unauthorized penetration.
- b. Construction is of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials resisting, and evidence of unauthorized entry into the area. If insert-type panels are used, a method is devised to prevent the removal of such panels without leaving visual evidence of tampering.
- c. The perimeter walls of the open storage area are true floor to ceiling, or, sufficiently modified to represent a secure enclosure. When wall barriers do not extend to the true ceiling and a false ceiling is created, walls are permanently constructed to extend above the false ceiling to the true ceiling using the same building materials as the existing walls.
- d. If there is a threat of forced entry (to include high crime areas) as determined by the physical security representative, walls are reinforced, slab-to-slab, with thirteen (13)-gauge expanded metal. The expanded metal is spot welded or fastened by M-40 approved method every 6 inches to vertical and horizontal metal supports of fourteen (14)-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.

5. Acoustic Controls

- a. Acoustic controls are designed to protect conversations from being overheard outside the OSAF. Acoustic controls are not intended to prevent a positive audio attack. OSAF perimeter walls, doors, windows, floors, and ceilings, as well as all openings such as vents and ducts, provide enough acoustic control measures to preclude inadvertent disclosure of conversation. This can be achieved through structural enhancements or sound masking if construction or budget restraints prevent structural enhancements from being feasible.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- b. The ability of an OSAF to retain sound within the perimeter is rated using a descriptive value, the STC. All OSAFs meet the equivalent of Sound Group III – STC of forty-five (45) or better. STC Group IV – STC of fifty (50) or better is required for amplified sound (e.g., secure video teleconferencing, speakerphone).
 - c. Sound Group III – STC of forty-five (45) or better. Loud speech from inside the room can be faintly heard but not understood from outside the room. Normal speech is unintelligible.
 - d. Sound Group IV – STC of fifty (50) or better. Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume can be heard only faintly or not all.
 - e. In certain cases, there may be sufficient stand-off distance between a perimeter wall and the operational area, to prevent sound from carrying beyond the perimeter wall. ODMNS may waive the STC construction requirement if the STC-45 equivalent rating can be achieved through stand-off distance. The stand-off distance is subject to inspection, and the area designated as a no-discussion area. Areas containing amplified sound are built out to an STC-50 equivalent sound rating.
 - f. Examples of sound masking include installation of noise generating systems that can be installed along the inside perimeter of the area. Where sound traverses through vents, ducts, and other similar openings, install music speakers in or near the opening, or white noise generators in or near the opening. When planning a retrofit, sound masking may be the most cost-effective option to meet the acoustic control requirements.
 - g. Examples of structural enhancements include the use of sound deadening high-density materials in wall construction; use of extra layers of drywall for wall construction; and use of door gaskets for doorframes. Where sound traverses through vents, ducts, and other similar openings, consider installing commercial sound baffles or waveforms. The installation of Z ducts is an effective method of protecting HVAC systems. When planning new construction, structural enhancements should be used to meet the acoustic control requirements.
 - h. Testing is performed after construction to ensure that the required STC level's equivalent has been met. The test is designed to ensure that CNSSI is protected from inadvertent disclosure and compromise. It is important that the test reflects the operational context of the area, the equipment to be deployed and the facilities' security-in-depth.
6. Radio Frequency (RF) Shielding
- a. RF shielding is not normally required in OSAFs unless otherwise required by the Certified Technical TEMPEST Authority (CTTA).

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

7. Intrusion Detection System (IDS)

- a. IDS and related Components comply with this Policy, the Underwriters Laboratories (UL) 2050 and Underwriters Laboratories (UL) 681 Extent 3 standards. Facilities maintain a current UL certificate (CRZH) of installation and services. The UL listed Alarm Service Company (ASC) is responsible for completing the National Industrial Security Alarm Description Worksheet.
- b. Certificate of Compliance. Evidence of compliance with the requirements of this Policy consists of a valid UL certificate for the appropriate category of service. This certificate is issued to the protected facility by UL, through the alarm installing company. The certificate serves as evidence that the alarm installing company is:
 - i. Listed as furnishing security systems of the category indicated;
 - ii. Authorized to issue the certificate of installation as representation that the equipment complies with requirements established by UL for the category of service;
 - iii. Subject to the UL Field Counter Check Program, whereby periodic inspections are made of representative alarm installations by UL-certified personnel to verify the correctness of installation practices.
- c. UL certificate (CRZH) exemptions

If the Component constructs and operates its own non-UL listed monitoring station, the Component Monitoring Station meets the construction and operational standards of a Government Contractor Monitoring Station as outlined in UL 2050. The IDS installation is accomplished by an alarm installation company that is certified by UL for 2050 compliance and the Component has a dedicated staff of trained Physical Security Technicians that provide everyday maintenance and repair of the IDS system.
- d. The IDS is connected to and monitored by; a UL listed monitoring station unless approved otherwise by ODMNS. The approval authority approves contingency protection procedures in the event of IDS malfunction.
- e. IDS requirements
 - i. Independent Equipment. When many alarmed areas are protected by one monitoring station, secure room zones are clearly distinguishable from the other zones to facilitate a priority response. All sensors are installed within the protected area.
 - ii. Premise Control Unit (PCU). No capability should exist to allow changing the access status of the IDS from a location outside the protected area without prior approval of the approval authority. All PCUs (alarm panel) is located inside the secure area. Assigned personnel initiate all changes in access and secure status. Operation of the PCU is restricted by use of a keypad and/or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space causes an alarm to be transmitted to the monitor station.

FOR OFFICIAL USE ONLY (FOUO)

- iii. Backup Power. Emergency backup electrical power is provided by battery, generator, or both. If batteries are used, the batteries provide a minimum of 24 hours of backup power.
- iv. Keypads. All alarm keypads are located inside the secure area next to the primary entry/exit door.
- v. Motion Detection Protection. Motion Detectors are a UL 639 listed device. Secure areas that reasonably afford access to the container or area where classified data is stored are protected with motion detection sensors (i.e., ultrasonic, passive infrared, etc.). Use of dual technology is authorized when one technology transmits an alarm condition independently from the other technology. All failed detector causes an immediate and continuous alarm condition.
- vi. Protection of Perimeter Doors. Each perimeter door is protected by a UL 634 listed Level 2, High Security Switch (HSS). The HSS removal tamper is monitored 24 hours a day regardless if the system is in the access or secure mode of operation.
- vii. Protection of Emergency Exit-Doors. Each perimeter Emergency Exit- Door is protected by a UL 634 listed Level 2, High Security Switch (HSS) and monitored 24 hours a day regardless if the system is in the access or secure mode of operation.
- viii. Entrance Door Delay. Entrance door sensors have an initial time delay to allow for change in alarm status, but not to exceed 30 seconds.
- ix. Windows. All readily accessible windows below 18 feet are protected by an appropriate intrusion detection unit installed to signal breakage or penetration of the window or movement of an intruder in the vicinity of the window. Additionally, a High Security Switch is used on windows that are movable.
- x. Duress. Minimum of one continuously alarmed duress button is recommended in all OSAFs.
- xi. False or Nuisance Alarm. Any alarm signal transmitted in the absence of a detected intrusion, or identified as a nuisance alarm, is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. All alarms are investigated, and the results documented. The maintenance program for the IDS should ensure that incidents of false alarms do not exceed one (1) in a period of thirty (30) days per zone.
- xii. The IDS is tested annually to provide assurance that the IDS system is in conformance with this Policy. US citizens accomplish all IDS testing.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- xiii. IDS PIN codes are FOUO and require additional protection from disclosure. The codes are not transmitted over unsecure phone lines or unencrypted/non-password protected email. Individual PIN codes are assigned to each user. Shared PIN codes are not authorized.

f. Central Monitoring Station.

- i. The central monitoring station may be located at the facility of a UL- listed:
 - 1. Government Contractor Monitoring Station, formerly called a proprietary central station;
 - 2. National Industrial Monitoring Station;
 - 3. Central Station that complies with the Standards for Central Station Alarm Services, UL 827; or
 - 4. Cleared Commercial Central Station.

NOTE: For the purpose of monitoring alarms, all provide an equivalent level of monitoring service.

- ii. U.S. Secret-cleared monitoring station employees are in attendance in enough numbers to monitor each alarmed area.
- iii. Trained alarm monitors are in attendance at the alarm monitoring station at all times when the IDS is in operation.
- iv. The central monitoring station is required to indicate whether the system is in working order and to indicate tampering with any element of the systems. Necessary repairs are made as soon as practical. Until repairs are completed, periodic patrols are conducted at four-hour intervals for Secret areas and two-hour intervals for Top Secret areas during non-working hours, unless an appropriately cleared employee is stationed at the alarmed site.
- v. When an IDS is used, it is activated immediately at the close of business at the alarmed area or container. A record is maintained to identify the person responsible for setting and deactivating the IDS. Each failure to activate or deactivate is reviewed by the central monitoring station and, upon appropriate determination, referred to the appropriate security official for investigation. Such records are maintained per the General Records Schedule.
- vi. Records are maintained for one year indicating time of receipt of alarm; name(s) of security force personnel responding; time dispatched to facility area; time security force personnel arrived; nature of alarm; and what follow-up actions were accomplished.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

g. Response to Alarms

- i. The following resources may be used to investigate alarms: proprietary security force personnel, central station guards, and subcontracted guard services.
- ii. When the IDS is in operation, enough trained proprietary security force personnel must be readily available. They must be cleared to the appropriate level of the area and should be immediately dispatched to investigate each alarm.
- iii. Response personnel is cleared only if they have the ability and responsibility to access the area or container(s) housing the classified material; i.e., keys to the facility have been provided or the personnel are authorized to enter the building or check the container or area that contains classified material.
- iv. Uncleared guards may be dispatched by a signaling service station, or residential monitoring station to an alarm. However, Component developed response plans include notification to a cleared representative of the affected facility for each alarm annunciation. If alarm activation resets in a reasonable amount of time and no physical penetrations of the area or container are visible, then entrance into the area or container is not required. The uncleared guards remain on the premises until a designated, cleared representative of the facility arrives, or as instructed by the cleared facility representative.
- v. If the alarm activation does not reset or physical penetration is observed, then a cleared response team is dispatched. The initial uncleared response team stays on station until relieved by the cleared response team.
- vi. Subcontracted guards are under contract with either the central monitoring station or the cleared facility.
- vii. The Component requires a 15-minute response time for TOP SECRET- level open-storage areas, and a 30-minute response time for SECRET-level open-storage areas. Arrangements are made with the monitoring station to immediately notify a cleared representative of the facility on receipt of the alarm. The representative is required to go immediately to the facility to investigate the alarm, and to take appropriate measures to secure the classified material.
- viii. The items listed below are some examples of security in-depth features. Security in-depth features are evaluated by SSO on a case-by-case basis.
 - A. Military installations, embassy compounds, or contractor compounds with a dedicated response force of U.S. persons. A Memorandum of Agreement (MOA) is executed outlining response requirements for these facilities.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- B. Enclosed vestibule outside of an OSAF entrance equipped with an approved high security lock and UL listed alarm equipment installed in accordance with manufacturer's instructions.
 - C. Separate building access controls/alarms along with elevator controls (e.g., after-hours card reader or PIN (with audit capability) required to gain access to building or elevator.
 - D. Fenced, alarmed compound with access-controlled vehicle gate and/or pedestrian gate.
- h. Exceptional Cases. If the requirements set forth above cannot be met due to extenuating circumstances, ODMNS approval may be requested for an alarm system that is:
- i. Monitored by a central control station but responded to by a local (municipal, county, state) law enforcement organization.
 - ii. Connected by direct wire to alarm receiving equipment located in a local (municipal, county, state) police station or public emergency service dispatch center. This alarm system is activated and deactivated by employees of the Component, but the alarm is monitored and responded to by personnel of the monitoring police or emergency service dispatch organization. Police department response systems may be requested only when ODMNS is in an area where:

Central control station services are not available with line security and/or proprietary security force personnel, or a contractually dispatched response to an alarm signal cannot be achieved within the time limits required.

It is impractical for the Component to establish a proprietary guard force at the location.

In these instances, an installation proposal, explaining how the system would operate, is submitted to ODMNS. The proposal includes enough justification for granting an exception and the full name and address of the police department that will monitor the system and provide the required response. The name and address of the UL-listed/UL- certified company that is installing the system, and inspecting, maintaining, and repairing the equipment is also furnished.

The facility requests a 15-minute response time from the police department for TOP SECRET-level open-storage areas and a 30-minute response time for SECRET-level open-storage areas. Arrangements are made with the monitoring station/police to immediately notify a cleared representative of the facility on receipt of the alarm. The representative is required to go immediately to the facility to investigate the alarm, and to take appropriate measures to secure the classified material.

In exceptional cases where central station monitoring service is available, but no proprietary security force of central station or subcontracted guard response is available, and where the

FOR OFFICIAL USE ONLY (FOUO)

police department does not agree to respond to alarms, and no other manner of response is available, ODMNS may approve cleared employees as the sole means of response.

- iii. Continuous Operations Facilities may not require an IDS. This type of secure area should be equipped with an alerting system if occupants cannot observe all potential entrances into the room. Duress devices may also be required.

ACCOUNTABILITY

With the exception of laptop computers processing classified information, and records of transmittal, inventories of classified documents are not required. However, the CCSO at his/her discretion may require Top Secret documents to be individually tracked and a signature record kept of those provided access. This is documented in component-specific standard operating procedures.

The following apply to all classified laptops:

- A. All classified laptops conform to the requirements set forth by the CIO for classified processing.
- B. Classified laptops are accounted for and discrepancies reported and investigated by the applicable security office and OIG as appropriate. An inventory of all laptops approved for the processing of classified information is maintained and updated twice per year. The inventory distinguishes those laptops that have been certified and accredited for use in classified processing from all other equipment maintained in the inventory. A copy of each completed inventory is provided to CISO.
- C. All Security Violations involving classified laptops are reported to CISO in accordance with Chapter 4 of this Policy. The servicing Security Official conducts or cause to be conducted a Preliminary Inquiry and/or Formal Investigation in accordance with Chapter 4 of this Policy. Security Violations involving SCI or SAP are also reported to CISO.
- D. Classified laptops, and unclassified laptops used within a classified environment, are labeled with the proper SF 700 series label or equivalent. SF 700 Series labels are ordered through the General Services Administration (GSA). The respective stock numbers are:
 - 1. SF 706, Top Secret, Stock No. 7540-01-207-5536
 - 2. SF 707, Secret, Stock No. 7540-01-207-5537
 - 3. SF 708, Confidential, Stock No. 7540-01-207-5538
 - 4. SF 710, Unclassified, Stock No. 7540-01-207-5539
 - 5. SF 712, SCI, Stock No. 7540-01-267-1158.
- E. Classified laptops are stored and transported in accordance to the procedures set forth in this Instruction.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- F. Laptops that process SCI or SAP information are protected and used in accordance with DCIDs 6/3 and 6/9, or successor directives.
- G. Classified laptops employ, as soon as practical, up-to-date encryption technology as stipulated by HUD MGMT/CIO. The employment of encryption does not lessen the standards for the safeguarding or storage of a classified laptop or relieve personnel of their responsibility to comply with such safeguarding or storage standards.

TRANSMISSION AND TRANSPORTATION

Classified information is transmitted and received pursuant to the standards cited in this Policy 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, aware of the transmission, and have the capability to properly safeguard it. Under no circumstances is classified information transmitted by any means other than the approved methods described in this Policy.

- A. TOP SECRET information is transmitted by:
 - 1. Direct contact between appropriately cleared persons.
 - 2. Secure telephone unit or equipment (STE) or Secure Fax keyed to the TOP SECRET level.
 - 3. DCS or other authorized government agency courier service.
 - 4. Department of State Courier System (also known as a diplomatic pouch).
 - 5. Electronic means over NSA-approved cryptographic communications system(s).
- B. SECRET and CONFIDENTIAL information is transmitted by any of the following means:
 - 1. Any of the methods approved for transmitting TOP SECRET.
 - 2. U.S. Postal Service Registered Mail.
 - 3. 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 are not used.
 - 4. Commercial carriers or cleared commercial messenger services cleared for such purpose under the National Industrial Security Program (NISPOM).

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

5. For overnight delivery within the U.S. and its Territories, the current holders of the General Services Administration (GSA) contract for overnight delivery of information for the Executive Branch may be used. The list of current holders of the GSA contract is updated and published periodically by CISO. When using these services, the following conditions apply:
 - a. Classified Communications Security (COMSEC) Information/Equipment, North Atlantic Treaty Organization (NATO), and FGI is not transmitted in this manner.
 - b. The use of street-side collection boxes is prohibited.
 - c. Carrier personnel are not notified that the package contains classified information.
 - d. Material is packaged for transmission as cited in Subsection G, below.
 - e. The outer address label may contain the personal name of the intended recipient.
 - f. The release signature block on the receipt label are not executed.
 - g. The sender is responsible for verifying the proper mailing address and ensuring that an authorized person is available to accept delivery.
 - h. Packages are shipped only on Monday through Thursday and not on the eve of a federal holiday unless prior arrangements have been made to ensure a cleared person is available to accept delivery.
- C. Under no circumstances is TOP SECRET information transmitted via the U.S. Postal Service or any other uncleared commercial delivery service. Questions concerning the transmission of TOP SECRET information, which are not covered in this Policy, are referred to the applicable local security official.
- D. Transmitting classified information to a U.S. 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, is 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 that the information does not at any time pass out of the control of a U.S. citizen and does not pass through a foreign postal system.
- E. Transmission of Classified Information to Foreign Governments.

The release of classified information to foreign governments is approved in accordance with HUD foreign disclosure policies and procedures.
- F. Shipment of Freight

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

1. Transmitting bulk classified material is performed by qualified, cleared carriers that are authorized to transport material via a Protective Security Service (PSS) under the Department of Defense Industrial Security Program. This may be used only within the United States when the size, bulk weight, and nature of the shipment make other methods impractical.
2. Observation is not required while the shipment is stored in an aircraft or ship in connection with flight or sea transmittal 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 is sealed to prevent access without detection.
3. 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 protects the shipment at all times, through personal observation, placing the shipment in protected storage, or other measures designed to prevent inspection, tampering, pilferage, or unauthorized access.
4. When additional control notices are imposed by an Original Classification Authority, the notices are honored when transmitting and transporting classified national security information.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

G. Preparation of Material for Transmission

1. All classified information physically transmitted outside government facilities is enclosed in two layers, both of which conceal the contents, prevent inadvertent opening, and provide reasonable evidence of tampering. When envelopes are used, the envelope is sealed with reinforced tape.
2. The inner enclosure clearly identifies 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.
3. The outer enclosure clearly identifies the office of the recipient (personal names are not used except as allowed for under Subsection B(5)(e), above), and the address 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 information 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 information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered to be a sufficient enclosure provided observation of it does not reveal classified information;
 - c. If the classified information is an item of equipment that is not reasonably packable and the shell or body is classified, it is concealed with an opaque enclosure that hides all classified features;
 - d. Specialized shipping containers, including closed cargo transporters or diplomatic pouches, may be considered the outer enclosure when used; and
 - e. When classified information is hand-carried outside a facility, a locked briefcase or similar locking container may serve as the outer enclosure.
4. CISO may approve the use of specialized shipping containers that are secured with a high security padlock, are equipped with an electronic seal that would provide evidence of surreptitious entry, are of sufficient construction to provide evidence of forced entry, and are handled by the carrier to ensure that the container is protected until its delivery is completed.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

H. Escort or Hand-Carrying of Classified Material

1. Courier Authorizations

Courier authorizations are issued to individuals who hand-carry classified information outside of, and beyond the perimeter of, a building or compound, and are processed through and approved by CCSO or CISO. Requests for courier authorization is submitted to the CCSO or CISO on DHS Form 11000-2, *Courier Authorization Request* (Appendix B). The individual's clearance level is equal to or exceeds the level of material being carried. Designated couriers are provided a briefing and/or briefing pamphlet by the security officer/liaison and acknowledge receipt of the briefing/pamphlet using the briefing acknowledgment form included at the end of the briefing pamphlet. The security officer/liaison retains the request form and acknowledgement form.

- a. A one-time courier letter is issued 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 thirty (30) days from the date of issue and may be issued by the CCSO or CISO or someone designated in writing by them for this purpose.
2. A permanent courier card is issued 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 (2) years from the date of issue. This may be requested through DHS Form 11000- 2, *Courier Authorization Request* (Appendix B).
 - a. Transporting classified materials aboard commercial aircraft is discouraged, and is approved by the CCSO or CISO only in instances of great urgency, and only when the materials cannot be transmitted by other means.
 - b. The request, with justification, is submitted to the CCSO or CISO using DHS Form 11000-2, *Courier Authorization Request* (Appendix B). The justification section clearly states that the courier is transporting classified information via commercial air.
 - c. If information technology equipment, e.g., a laptop computer, computer media, etc., containing classified information is to be transported, it is encrypted prior to transport.
 - d. The CCSO or CISO approves or disapproves the request based on the justification provided.
 - e. If approved, a courier authorization letter is prepared and issued by the CCSO or CISO.
3. Transport of Classified Material Within an Activity or Office
 - a. If required to transport classified material from one building to another via a public street or road, courier authorization is required, and the material is packaged in accordance with the requirements of this Instruction.

FOR OFFICIAL USE ONLY (FOUO)

- b. If required to transport classified material within the same building or compound, an appropriate cover sheet is affixed to the document and the document is placed in an unmarked envelope or folder to avoid undue attention. Courier authorization is not required.

4. International Transport

When necessary to hand-carry classified information outside of the U.S., every effort is made to use the Department of State Courier System. All other requests are decided on a case-by-case basis by CCSO/CISO.

I. Receipts

Components implement procedures to ensure timely notification of receipt for TOP SECRET and SECRET materials transmitted or transferred outside a component. SF 135-85b, *Records Transmittal and Receipt* (Appendix B), will be used for this purpose. With the exception of certain categories of information, e.g., NATO and FGI, and materials transmitted to a cleared contractor, receipts for CONFIDENTIAL materials are at the discretion of the sender.

REPRODUCTION

Reproduction of Classified Material. Documents and other materials containing classified information are reproduced only when necessary to accomplish the mission of the organization, or for compliance with applicable statutes or directives. Since reproduction equipment and the reproduction process involve substantial risk, HUD components establish and enforce procedures for reproduction of classified information that limits reproduction to that which is mission-essential and ensures that appropriate countermeasures are taken to negate or minimize risk. The use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is encouraged.

- A. Approval for Reproduction. Unless restricted by the originating agency, TOP SECRET, SECRET, and CONFIDENTIAL information may be reproduced to the extent required by operational needs. Components establish procedures that, at a minimum:
 - 1. Ensure compliance with reproduction limitations placed on documents by originators and special controls applicable to SAPs and other special categories of information;
 - 2. Facilitate oversight and control of reproduction of classified material; and,
 - 3. Control Procedures. Components establish controls to ensure that:
 - a. Reproduction is kept to a minimum consistent with mission requirements;

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- b. Classified material is not reproduced on equipment that poses unacceptable risks, for example, machines that are connected to an unclassified LAN, equipped with remote diagnostics, equipped with an internal memory, or in some other way retain images;
- c. Personnel doing the reproduction are aware of the risks involved with the specific reproduction equipment and the appropriate countermeasures they are required to take;
- d. Reproduced material is clearly identified as classified at the applicable level;
- e. Reproduced material is placed under the same accountability and control requirements as apply to the original material; and
- f. Waste products generated during reproduction are properly protected and disposed of.

DISPOSITION AND DESTRUCTION OF CLASSIFIED MATERIAL

- A. Classified documents and other materials are retained within HUD only if the documents are required for effective and efficient operation of the organization, or if law or regulation requires retention. Documents that are no longer required for operational purposes are 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. Destruction of classified documents and materials is accomplished by means that eliminate risk of reconstruction of the classified information the documents contain.
- B. Components ensure that retention management of classified information is included in oversight and evaluation of program effectiveness.
- C. Methods and Standards
 - 1. Classified information identified for destruction is destroyed completely to preclude recognition or reconstruction of the classified information. Methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition, or pulverizing.
 - 2. Cross-cut shredders currently in use that produce a residue particle size that does not exceed 1/32 inch in width by 1/2 inch in length may continue to be used for the destruction of classified information based upon the provided disposition from the Originator or until and if Federal requirements change. 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 complies with CNSS Policy No. 16, *National Policy for the Destruction of COMSEC Paper Material*, and is equipment listed on the National Security Agency (NSA) Evaluated Products List (EPL) of High Security Crosscut

FOR OFFICIAL USE ONLY (FOUO)

Shredders. A copy of the EPL can be obtained by calling the NSA National Information Assurance Center at (800) 688-6115. Technical guidance on other methods of destruction can be obtained by contacting HUD OSEP.

3. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media, processing equipment components, and the like may be obtained by contacting the Directorate for Information Systems Security, National Security Agency through OCAO SSO.

ALTERNATIVE CONTROL MEASURES AND WAIVERS

- A. The CCSO/CISO may approve the use of alternative security controls or measures to ensure that the protection afforded classified information is sufficient to reasonably deter and detect actual or possible compromise. Approval to use alternative control measures is submitted to the OCAO SSO who may authorize a waiver.
- B. Alternative security control measures are employed only when the minimum standards in this Policy cannot be met, and after considering risk management factors such as criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated, vulnerability to exploitation, and countermeasures benefits versus cost.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CHAPTER 5: SECURITY VIOLATIONS AND INFRACTIONS

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

Incidents involving SCI, SAP information, and/or COMSEC information are reported and investigated within the specific channels established for these types of information. At a minimum, such incidents are reported to the appropriate Component, SAP Security Officer, or COMSEC Manager, as applicable.

Incidents involving contractors, grantees, licensees, and other personnel falling under the purview of the National Industrial Security Program (NISP) are handled in accordance with this Policy and the National Industrial Security Program Operating Manual (NISPOM).

REPORTING A SECURITY INCIDENT

- A. Protecting classified information is of paramount concern upon discovery of any security incident. When an incident is discovered, immediate action is taken to secure and control any classified information involved.
- B. Security Incidents are reported promptly, but no later than the next business day from time of discovery, to the CCSO or to CISO. DHS Form 11000-11, *Record of Security Violation* (Appendix B), is used for this purpose.
- C. Any Security Incident that results in the compromise of classified information or that involves a Security Officer (as defined above); or a senior HUD Official to include a political appointee; a flag officer; a senior executive service or senior intelligence service employee; or involves the possible or actual compromise of classified information to a foreign national or foreign entity is reported to CISO. This may be reported by emailing HUD.SSO@hud.gov or anonymously to:

Department of Housing and Urban Development
Special Security Officer
451 7th St SW, Room 6282
Washington, D.C. 20410

- D. Pursuant to EO 13526, CISO reports applicable violations to the OCAO SSO.

REPORTABLE SECURITY INCIDENTS

Security Incidents that are reported and for which a Preliminary Inquiry and/or Formal Investigation is conducted 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.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- B. Any knowing, willful or negligent action to classify or continue the classification of information contrary to the requirements of EO 13526, and its implementing directives.
- C. Any knowing, willful, or negligent action to create or continue a SAP contrary to the requirements of EO 13526.
- D. Any incident involving computer or telecommunications equipment or media that may result in disclosure of classified information to unauthorized individuals, or that results in unauthorized modification or destruction of classified system data, loss of classified computer system processing capability, or 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 shipment 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 not authorized access.
- I. Any incident in which classified information has been destroyed by unauthorized means.
- J. Any incident in which classified information has been reproduced without authorization or contrary to specific restrictions imposed by the originator.
- K. Any other incident in which classified information is not safeguarded or handled in accordance with prescribed procedures.

SECURITY INQUIRIES

- A. Upon notification of an alleged Security Incident, CCSO or CISO initiates or causes to be initiated a Security Inquiry. The person conducting the Security Inquiry serves as the Inquiry Official. The Inquiry Official has the authority to conduct interviews and obtain statements from personnel knowledgeable about the incident.
- B. Should the alleged Security Incident involve a CCSO or his or her supervisor, the issue is referred to CISO to conduct the Security Inquiry (contact information above).
- C. The Security Inquiry and corresponding Report of Inquiry are completed within fifteen (15) work days from date of initiation. Where an inquiry cannot be completed within fifteen (15) work days, the Inquiry Official includes a statement in the Report of Inquiry justifying the delay.

FOR OFFICIAL USE ONLY (FOUO)

- D. The Security Inquiry is conducted to determine and the subsequent report includes:
1. Whether a Security Violation or a Security Infraction occurred;
 2. Time, date, and location of the incident;
 3. Whether there was a compromise or suspected compromise of classified information and identification of the classified information involved;
 4. The person(s) responsible for and involved in the Security Violation or Infraction;
 5. The cause of the Security Violation or Infraction;
 6. The actions taken to minimize damage or neutralize the potential for compromise; and
 7. Recommendations to prevent recurrence of similar Security Incidents, to include additional training, procedural changes, and/or action.
- E. If the Security Incident involves the improper transmission of classified information to HUD from another agency, the appropriate Security Official of the sending office or agency is notified by the local HUD security official for further action in accordance with that agency's regulations.
- F. If the Security Incident involves the improper transmission of classified information within HUD, the appropriate Security Official of the sending Component is notified for further action in accordance with this Policy.
- G. If the Security Inquiry reveals a compromise or a suspected compromise of classified information, the CCSO or CISO requests that the OCA with jurisdiction over the information conduct a Damage Assessment.
1. If the compromised information was originated by an OCA, the Security Inquiry Report and request for Damage Assessment is forwarded to CISO for processing.
 2. If the compromised information was originated by another government agency, a copy of the Security Inquiry Report and request for Damage Assessment is forwarded to the applicable government agency. A copy of the Security Inquiry Report and request for Damage Assessment is forwarded to CISO.
 3. If the originator of the information cannot be determined, the Security Inquiry Report is forwarded to CISO. CISO attempts to determine the originator of the information and processes the Damage Assessment request. If CISO cannot determine the originator, CISO seeks guidance from the OCAO SSO.

FOR OFFICIAL USE ONLY (FOUO)

- H. If the incident involves the inadvertent disclosure of classified information to a person not authorized access, then the person who received the information is asked to sign an *Inadvertent Disclosure Statement*. If the person refuses to sign the Inadvertent Disclosure Statement, the information on the form is read orally to the person in the presence of a witness, and the form annotated to reflect the individual's refusal to sign; both the Inquiry Official and the witness sign the form. This information is included in the Security Inquiry Report.
- I. The completed Security Inquiry Report is forwarded to the official(s) with jurisdiction over the office or agency where the Security Incident occurred and the person(s) involved for further action as appropriate.
- J. If the Security Inquiry Report contains classified information, it is handled and marked accordingly. At a minimum, the Security Inquiry Report is marked and handled as "For Official Use Only" in accordance with Management Directive 11042.1, or its successor Instruction.
- K. Persons found to have committed a Security Violation or Infraction are afforded the opportunity to provide a written statement disputing the facts or identifying mitigating circumstances. Such written statements are included as an attachment to the Security Inquiry Report.
- L. A copy of the Security Inquiry report is retained by the applicable security office in accordance with records retention guidelines. When a person(s) is found to have committed a Security Violation or Infraction, a copy of the Security Inquiry Report is also be included in the individual's Personnel Security File. Upon receipt, the applicable Personnel Security Office reviews the report to determine if suspension or revocation of a security clearance is appropriate. Reports pertaining to contract employees are provided to the applicable Federal Contracting Officer's Technical Representative, or equivalent Federal employee having oversight of the contract. In addition, further reporting relative to contractors is made in accordance with the [National Industrial Security Program Operating Manual](#).
- M. A Security Inquiry is sufficient to close the incident if it is determined that:
 - 1. The loss or compromise of classified information has not occurred or its likelihood is remote;
 - 2. The compromise of classified information has occurred but there is no indication of knowing, willful, or negligent behavior or significant security weaknesses;
 - 3. There is no evidence of employee misconduct, criminal behavior, or espionage; and
 - 4. No additional information is likely to be obtained by conducting a Formal Investigation.

FORMAL INVESTIGATION

- A. The decision to conduct a Formal Investigation in lieu of or subsequent to a Security Inquiry is made by the CCSO or CISO.

FOR OFFICIAL USE ONLY (FOUO)

- B. Upon determination that a Formal Investigation is appropriate, the matter is referred to the appropriate investigative entity. The Formal Investigation is conducted by officers or agents with appropriate legal authority to conduct investigations into violations of law, to include persons with law enforcement authority or credentialed employees of an OPR, OIG, or similar investigative entity. ROI are prepared in accordance with the guideline established by the investigating agency. Should the OIG, the Federal Bureau of Investigation, or another agency assume investigative responsibility, HUD Components coordinate any further actions with that investigative agency.
- C. A copy of the completed ROI is forwarded to CISO by the investigative agency.

INCIDENTS INVOLVING CLASSIFIED INFORMATION WITHIN INFORMATION TECHNOLOGY (IT) SYSTEMS (CLASSIFIED SPILLAGE)

- A. The accidental, inadvertent, or intentional introduction of classified information into an IT system 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, is reported to the cognizant local security official. Immediate action is taken to assess and mitigate the incident. Assessment includes an immediate determination as to whether or not a spill occurred, e.g., is the information introduced to the IT system classified or classified at a higher level than what the IT system is certified and accredited to process.
- B. When a determination is made that a spill occurred, the reporting requirements outlined in this Policy are followed.
- C. Users 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 off on a printer.
- D. Specific information regarding a spill is itself classified at the same level of the classification of the information spilled until confirmation is received that the spilled information was effectively eradicated from the IT system or the potential for compromise was otherwise neutralized. Specific information means information sufficient to allow a dedicated intruder or curiosity seeker to search for and access the spilled material.
- E. The conduct of a Security Inquiry and/or Formal Investigation proceeds in accordance with this Policy.

SECURITY VIOLATIONS AND INFRACTIONS IN FOREIGN COUNTRIES

- A. Security Incidents occurring in foreign countries are under the purview of the Department of State (DOS). If a Security Incident is observed by HUD personnel in a foreign country, the DOS Regional Security Officer(s), United States Marine Corps (USMC) Security Guard(s) or other designated person(s) are notified.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- B. Security Incidents occurring in foreign countries involving HUD personnel are reported by DOS to CISO using an OF 117, *Notice of Security Violation*.
- C. Upon receipt of OF 117, CISO forwards the notice, with a cover letter, to the applicable CCSO for further action.

OTHER AGENCY SECURITY VIOLATIONS AND INFRACTIONS

- A. HUD personnel who observe or learn of a Security Incident committed by a visiting or detailed employee or contractor of another agency follow the guidelines provided in this Instruction for reporting and conducting a Security Inquiry or Formal Investigation.
- B. The CCSO or CISO sends a memorandum to the security office of the visiting or detailed individual's agency with a description of the incident.

SANCTIONS

- A. When an individual is found to be responsible for the commission of a Security Violation or Infraction, he/she may be subject to administrative, disciplinary, or criminal sanctions. The type of sanctions imposed is based on several considerations, including the following:
 - 1. Severity of the incident;
 - 2. Intent of the person committing the Security Violation or Infraction;
 - 3. Extent of training the person(s) has received;
 - 4. Frequency of which the individual has been found responsible in the commission of other such Security Violations or Infractions.
- B. 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.
- C. Administrative sanctions are assessed in accordance with the policies, procedures, and practices established by OCHCO within the Component, and actions involving the suspension or revocation of a security clearance are taken in accordance with the applicable EOs and ODNI policies and regulations.
- D. Where a proposed sanction associated with the unauthorized disclosure of classified information is in excess of a reprimand, the matter is coordinated with OGC. Further, where a criminal violation has occurred that may result in a criminal prosecution, the matter is coordinated with OGC and the DOJ.
- E. The applicability of sanctions is determined without consideration of rank or position.

FOR OFFICIAL USE ONLY (FOUO)

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CHAPTER 6: CLASSIFIED FGI

GENERAL

Information classified by a foreign government is generally treated the same as its U.S. equivalent. In certain circumstances, information may be protected as “Confidential Modified Handling” to mimic foreign classification systems when those systems provide for classification below that of U.S. Confidential. Unless otherwise subject to statute, treaty, or other international agreement, classified FGI within HUD is handled in accordance with this Policy.

CLASSIFICATION

- A. Information classified by a foreign government retains its original classification markings or is assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. FGI retaining its original classification markings need not be assigned a U.S. classification marking provided that the foreign government markings are adequate to meet the purposes served by U.S. classification markings. Otherwise, documents are marked, “This document contains (insert name of country) (insert classification level) information to be treated as U.S. (insert classification level).”
- B. Some foreign government classification regimes have a level below that of U.S. Confidential (i.e., “Restricted,” or “Designated”). In these cases, the information is protected in a manner equal to the protection provided by the foreign government. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information. When a lesser standard than U.S. Confidential is used, the notation, “Modified Handling Authorized” may be added.
- C. FGI that has not been classified by the originating foreign government but that has been provided to the U.S. with the expectation that it will be held in confidence, may be classified by an OCA if it otherwise meets the classification standards cited in EO 13526. In such instances, the information may be classified by the OCA as “Confidential/Modified Handling Authorized.” Information falling into this category is classified information but it may be protected at a lesser standard than other U.S. Confidential information to achieve equivalency in the protection standards provided by the originating foreign government.

DECLASSIFICATION

Unless subject to statute, treaty, or other international agreement, the limits on the duration of classification are applicable to classified FGI. When FGI appears subject to automatic declassification, HUD determines whether the information is subject to statute, treaty, or international agreement that would prevent its declassification at the time. HUD also determines if another exemption under 3.3(b) of EO 13526, such as the exemption that pertains to United States foreign relations, may apply to the information. As appropriate, HUD also consults with DOS prior to declassification.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

ACCESS

Access to information protected as “Confidential Modified Handling Authorized” requires a need-to-know; however, a security clearance is not required. Access to FGI that possesses a classification equivalent to a U.S. classification is controlled in the same manner as access to the equivalent U.S. level of classification.

STORAGE

Classified FGI is stored in the manner equivalent to the respective U.S. classification. To the extent practical, and to facilitate its control, FGI is stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. Information protected as “Confidential Modified Handling Authorized” is stored in such a way as to preclude unauthorized access, such as a locked drawer or file cabinet. A GSA approved safe, while encouraged, is not required.

TRANSMISSION

Information protected as “Confidential Modified Handling Authorized” is still classified information and may only be transmitted, to include electronic means, via a method approved for U.S. Confidential information. This requirement may be waived by the originating government (i.e., to allow the use of unsecured phones and/or government unclassified email). Information that has been classified by a foreign government is transmitted in a manner equivalent to the respective U.S. classification.

TRANSFER

If required by treaty, agreement, bilateral exchange, or other obligation, FGI is not released or disclosed to a third country entity without approval of the originating government..

ACCOUNTABILITY AND REPRODUCTION

FGI requires the following accountability and reproduction controls beyond that prescribed for classified U.S. information:

A. Top Secret

Records are maintained of the receipt, internal distribution, destruction, access, reproduction and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction is witnessed.

B. Secret

Records are maintained of the receipt, external dispatch and destruction of foreign government Secret information. Other records may be required as determined by the originator. Reproduction is permitted consistent with mission need unless prohibited by the originator. Reproduction is recorded unless this requirement is waived by the originator.

C. Confidential

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

Records need not be maintained unless required by the originator.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CHAPTER 7: MARKING

GENERAL

The following are applicable to all classified documents:

- A. Markings are applied according to the requirements of EO 13526, 32 CFR part 2001, and the guidance provided in the ISOO pamphlet “Marking Classified National Security Information.” These requirements and any supplemental markings are implemented in accordance with this Chapter or current CAPCO standards.
- B. The cover, first page, and title page (if any) are prominently marked at the top and bottom of the page with the highest classification of information contained within the document.
- C. Either the highest classification of information in the document or on the page is prominently marked on the top and bottom of every page.
- D. A classification block is located so that it is immediately apparent on the cover page or first page. It indicates the person who created the document along with his or her title and office, or, if assigned a personal identifier, the basis for the classification, and a declassification instruction.
- E. 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) is portion marked to indicate the highest level of classification in the marked portion.
- F. Portion markings are (TS) for Top Secret, (S) for Secret, (C) for Confidential, and (U) for Unclassified.
- G. The date of the document is readily apparent.
- H. When marking documents that are classified by compilation, any unclassified portions are 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 appear with the compiled information to indicate when individual portions constitute a classified compilation and when the individual portions do not.

ORIGINALLY CLASSIFIED DOCUMENTS

In addition to the preceding requirements, the classification block of an originally classified document in which the decision has not yet been incorporated into a security classification guide is as follows:

Classified by: (Name, Position, and Office)

Reason: (Applicable reason as cited in section 1.4 of EO 13526, e.g., 1.4(g))

Declassify on: (date or event not to exceed twenty-five (25) years)

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

DERIVATIVELY CLASSIFIED DOCUMENTS

- A. In addition to the requirements in Section 1, the classification block of a derivatively classified document is as follows:

Classified by: (Name, Position and Office of Origin (if not otherwise evident) or personal identifier)

Derived from: (Identity of source documents)

Declassify on: (Date or event as reflected on the source)

- B. If the document is derived from multiple sources, this is indicated in the “Derived From” line, and a listing of the classified sources is identified in 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.
- C. Declassification Instructions
1. When displayed numerically, it is marked in the format YYYYMMDD. Spelling out or abbreviating the month (e.g., January 1, 2011 or Jan 1, 2011) is also acceptable.
 2. When using multiple sources, the declassification instruction applied is the most restrictive declassification date or event from the sources.
 3. Except for documents with the 50X1-Human or 50X2-WMD exemptions, documents using approved declassification exemptions (e.g., 25X7, 25X8, etc.) always include the ISCAP approved declassification date or event that accompanies the exemption.
 4. When a document is classified by either a source document or classification guide in which the declassification instruction is OADR, MR, or X1, X2, X3, X4, X5, X6, X7, or X8, the derivative classifier calculates a date twenty-five (25) years from the date of the source document for use as the declassification instruction for the newly created document.
 5. If a source document is marked with the declassification instruction, “DNI Only” or “DCI Only” and does not contain information described in EO 12951, *Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems*, the derivative classifier calculates a date that is twenty-five (25) years from the date of the source document for use as the declassification instruction for the newly created document.
 6. If a document is marked with “DCI Only” or “DNI Only” and the information is subject to EO 12951, the derivative classifier uses “25X1, EO 12951” or other declassification instruction prescribed by the DNI.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

D. Documents Containing RD and/or FRD Information.

In addition to the marking requirements in Section 1, a RD Derivative Classifier marks or authorizes the marking of a document containing RD and/or FRD information with the following markings in addition to the classification level:

1. Front Page/Title Page Markings. In addition to the overall classification level of the document (i.e., Top Secret, Secret, Confidential), one of the following notices appears on the front of the document:

If the document contains RD information:

RESTRICTED DATA

This document contains RESTRICTED DATA
as defined in the Atomic Energy Act of 1954.

Unauthorized disclosure subject to
administrative and criminal sanctions.

If the document contains FRD information, but not RD:

FORMERLY RESTRICTED DATA

Unauthorized disclosure subject to
administrative and criminal sanctions. Handle
as RESTRICTED DATA in foreign
dissemination.

Section 144b, Atomic Energy Act of 1954.

2. Declassification Instructions for RD/FRD

For documents containing wholly RD or FRD, the declassification instruction is marked, “Not Applicable” or “N/A.” When RD or FRD is comingled with other classified information, the instruction reads, “Not applicable to RD/FRD portions, see source listing for NSI portions.” The source listing then contains the declassification instructions for each non-RD/FRD classified source. However, in these instances, no source declassification date or event appears on the front page of the document.

3. Interior Page Markings. Each interior page of the document is clearly marked at the top and bottom of the page with the overall classification level and category of the document or the classification level and category of the information on that page, whichever is preferred (e.g., SECRET- RESTRICTED DATA). The abbreviations “RD” and “FRD” may be used in conjunction with the interior page classification level (e.g., SECRET-RD).

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

4. Portion Markings. Portion markings are not required on RD documents, even if the documents also contain NSI. However, RD documents can be portion marked at the discretion of the RD Derivative Classifier. The markings are placed immediately preceding the portion to which the markings pertain and contain both the level and category of information contained in the portion. Unless portion marked, documents that comingle RD/FRD and other classified information are not used as a source for non-RD/FRD documents.

E. Documents containing NATO information

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

1. The abbreviations for portion markings are as follows:

Cosmic Top Secret ATOMAL (CTSA)
Cosmic Top Secret (CTS)
NATO Secret ATOMAL (NSA)
NATO Secret (NS)
NATO Confidential ATOMAL (NCA)
NATO Confidential (NC)
NATO Restricted (NR)
NATO Unclassified (NU).

2. NATO Unclassified Information only requires portion markings when it is part of a larger document intermixing NATO classified information or non-NATO information.
3. Declassification instructions may not be present. This is especially true if the information is not U.S. generated. In instances where a document is wholly NATO and no declassification instruction is given, the declassification instruction is "Not Applicable" or "N/A." In instances where NATO information is comingled with national security information, the declassification instruction is "Not applicable to NATO portions, see source listing for NSI portions." The source list then includes the declassification instructions for each source.
4. NATO information is not subject to automatic declassification. Questions on the classification of NATO information are referred to the CUSR, through OS. Original information generated by HUD for release to NATO has a declassification date in accordance with EO 13526.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

F. Documents containing FGI

1. FGI retaining its original classification markings need not be assigned a U.S. classification marking provided that the foreign government markings are adequate to meet the purposes served by U.S. classification markings. Otherwise, the documents are marked, “This document contains (insert name of country) (insert classification level) information to be treated as U.S. (insert classification level),” and pertinent portions are marked ‘FGI’ together with the classification level, e.g., (FGI-C).
2. Some foreign government classification regimes have a level below that of U.S. Confidential (i.e., “Restricted,” or “Designated”). In these cases, protection equal to that provided by the foreign government needs to be ensured. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information. When a lesser standard than U.S. Confidential is used, the notation, “Modified Handling Authorized” may be added (portion marking: //FGI –CMOD, where FGI is replaced with the trigraph of the originating country).

WORKING PAPERS

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

- A. Release outside of the originating office or activity
- B. Retained more than 180 days from the date of origin
- C. Filed permanently

TRANSMITTAL DOCUMENTS

A transmittal document indicates on its face the highest classification level of any classified information attached or enclosed. The transmittal also includes conspicuously on its face 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).

OTHER MATERIALS

Bulky material, equipment, and facilities are clearly identified in a manner that leaves no doubt about the classification status, the level of protection required, or the duration of classification. Upon a finding that

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

identification would itself reveal classified information (such as a covert facility), such identification is not required; however, documentation of such is maintained by the cognizant security office.

DECLASSIFICATION MARKINGS

Declassified materials are marked with the word, “Declassified.” All classification markings such as headers, footers, and portion markings are lined through. The front page identifies by name, position, or personal identifier the authority for declassification as cited in Chapter 2, Section 6.C., and where applicable, a declassification guide identified by title and date.

ELECTRONIC MARKINGS

A. Classified information in the electronic environment is:

1. Subject to all requirements of EO 13526.
2. Marked with proper classification markings to the extent that such marking is practical, including portion marking, overall classification, “Classified By,” “Derived From,” “Reason” for classification (originally classified information only), and “Declassify On.”
3. Marked with proper classification markings when appearing in an electronic output (e.g., database query) in which users of the information need to be alerted to the classification status of the information.
4. Marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the original classification authority. In cases where classified information in an electronic environment cannot be marked in this manner, a warning is applied to alert users that the information may not be used as a source for derivative classification. Additionally, a point of contact and instructions for users to receive further guidance on the use and classification of the information is provided.
5. Prohibited from use as source of derivative classification if it is dynamic in nature (e.g., wikis and blogs) and not marked in accordance with the EO.

B. Markings on classified e-mail messages.

1. E-mail transmitted on or prepared for transmission on classified systems or networks is configured to display the overall classification at the top and bottom of the body of each message. The overall classification marking string for the e-mail reflects the classification of the header and body of the message. This includes the subject line, the text of the e-mail, a classified signature block, attachments, included messages, and any other information conveyed in the body of the e-mail. A single linear text string showing the overall classification and markings is included in the first line of text and at the end of the body of the message after the signature block.

FOR OFFICIAL USE ONLY (FOUO)

2. Classified e-mail is portion marked. Each portion is 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 is 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.
3. A classified signature block is portion marked to reflect the highest classification level markings of the information contained in the signature block itself.
4. Subject lines are portion marked to reflect the sensitivity of the information in the subject line itself and do not reflect any classification markings for the e-mail content or attachments. Subject lines and titles are portion marked before the subject or title.
5. For a classified e-mail, the classification authority block is placed after the signature block, but before the overall classification marking string at the end of the e-mail. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.
6. When forwarding or replying to an e-mail, individuals ensure that in addition to the markings required for the content of the reply or forwarding e-mail itself, the markings reflect the overall classification and declassification instructions for the entire string of e-mails and attachments. This includes any newly drafted material, material received from previous senders, and any attachments.

C. Marking web pages with classified content.

1. Web pages are classified and marked based upon the content on the pages, regardless of the classification of the pages to which the web pages link. Any presentation of information to which the web materials link is also marked based on its own content.
2. The overall classification marking string for every web page reflects the overall classification markings (and any dissemination control or handling markings) for the information on that page. Linear text appearing on both the top and bottom of the page is acceptable.
3. If any graphical representation is utilized, a text equivalent of the overall classification marking string is included in the hypertext statement and page metadata. This enables users without graphic display to be aware of the classification level of the page and allows for the use of text translators.
4. Classified web pages are portion marked. Each portion is marked to reflect the highest level of information contained in that portion. A portion containing a URL or reference to another document is portion marked based on the classification of the content of the URL itself, even if the content to which it points reflects a higher classification marking.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

5. Classified web pages include the classification authority block on either the top or bottom of the page. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.
6. Electronic media files such as video, audio, images, or slides carry the overall classification and classification authority block, unless the addition of such information would render the files inoperable. In such cases, another procedure is used to ensure recipients are aware of the classification status of the information and the declassification instructions.
7. Marking classified URLs. URLs provide unique addresses in the electronic environment for web content and are portion marked based on the classification of the content of the URL itself. The URL is not portion marked to reflect the classification of the content to which it points. URLs are developed at an unclassified level whenever possible. When a URL is classified, a classification portion mark is used in the text of the URL string in a way that allows identification of the URL as a classified portion in any textual references to that URL. An example may appear as:

[http://www.center.xyz/SECRET/filename \(S\).html](http://www.center.xyz/SECRET/filename (S).html)

[http://www.center.xyz/filename2 \(TS\).html](http://www.center.xyz/filename2 (TS).html)

[http://www.center.xyz/filename \(TS//NF\).html](http://www.center.xyz/filename (TS//NF).html)

D. Marking classified dynamic documents and relational databases.

1. A dynamic page contains electronic information derived from a changeable source or ad hoc query, such as a relational database. The classification levels of information returned may vary depending upon the specific request.
2. If there is a mechanism for determining the actual classification markings for dynamic documents, the appropriate classification markings are applied to and displayed on the document. If such a mechanism does not exist, the default is the highest level of information in the database, and a warning is applied at the top of each page of the document. Such content is not used as a basis for derivative classification. An example of such an applied warning may appear as:

This content is classified at the [insert system-high classification level] level and may contain elements of information that are unclassified or classified at a lower level than the overall classification displayed. This content may not be used as a source of derivative classification; refer instead to the pertinent classification guide(s).

This alerts users of the information that there may be elements of information that may be either unclassified or classified at a lower level than the highest possible classification of the information returned. Users are encouraged to make further inquiries concerning the status of individual elements in order to avoid unnecessary classification and/or impediments to information sharing. Resources such as classification guides and points of contact are established to assist with these inquiries.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

3. Users developing a document based on query results from a database properly mark the document in accordance with 32 CFR § 2001.22. If there is doubt about the correct markings, users contact the database originating agency for guidance.

E. Marking classified bulletin board postings and blogs.

1. A blog, an abbreviation of the term “web log,” is a website consisting of a series of entries, often commentary, description of events, or other material such as graphics or video, created by the same individual like a journal, or created by many individuals. While the content of the overall blog is dynamic, entries are generally static in nature.
2. The overall classification marking string for every bulletin board or blog reflects the overall classification markings for the highest level of information allowed in that space. Linear text appearing on both the top and bottom of the page is acceptable.
3. Subject lines of bulletin board postings, blog entries, or comments is portion marked to reflect the sensitivity of the information in the subject line itself, not the content of the post.
4. The overall classification marking string for the bulletin board posting, blog entry, or comment reflects the classification markings for the subject line, the text of the posting, and any other information in the posting. These strings are entered manually or by utilizing an electronic classification tool in the first line of text and at the end of the body of the posting. These strings may appear as single linear text.
5. Bulletin board postings, blog entries, or comments are portion marked. Each portion is marked to reflect the highest level of information contained in that portion.

F. Marking classified wikis.

1. Initial wiki submissions include the overall classification marking string, portion marking, and the classification authority block string in the same manner as mentioned above for bulletin boards and blogs. All of these strings may appear as single line text.
2. When users modify existing entries which alter the classification level of the content or add new content, they change the required markings to reflect the classification markings for the resulting information. Systems provide a means to log the identity of each user, the changes made, and the time and date of each change.
3. Wiki articles and entries are portion marked. Each portion is marked to reflect the highest level of information contained in that portion.

G. Instant messaging, chats, and chat rooms.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

1. Instant messages and chat conversations generally consist of brief textual messages but may also include URLs, images, or graphics. Chat discussions captured for retention or printing are marked at the top and bottom of each page with the overall classification reflecting all of the information within the discussion and, for classified discussions, portion markings and the classification authority block string also appear.
 2. Chat rooms display system-high overall classification markings and contain instructions informing users that the information may not be used as a source for derivative classification unless it is portion marked, contains an overall classification marking, and a classification authority block.
- H. Attached files. 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 OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CHAPTER 8: SECURITY EDUCATION, TRAINING, AND AWARENESS (SETA) PROGRAM

GENERAL

A. The SETA program includes, but is not limited to, the development and presentation of the following:

1. Security Orientation Briefing

All Federal employees, to include contractor employees, consultants, and detailed personnel are required to attend a Security Orientation Briefing within the first thirty (30) days of assignment. It is only necessary to attend Security Orientation one time.

2. Initial Security Briefing

An initial security briefing is provided to all HUD personnel who have met the standards 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 or another OSEP person assisting with the briefing, and submitted to the individual's component Personnel Security division for filing in his/her permanent personnel security file. An individual is only required to sign a SF-312 once unless he/she has been debriefed, or his/her clearance has been administratively withdrawn; in which case he/she receives another briefing and a new SF-312 is signed prior to receiving access.

3. Annual Refresher Training

Annual refresher briefings are mandatory for all HUD employees to reinforce and update awareness of security policies and to reinforce the employees' responsibilities. All personnel who handle or generate classified information and/or hold a security clearance complete the Annual Refresher for Clearance Holders briefing; all others complete the Annual Refresher for Non-clearance Holders. Annual refresher training also addresses: (1) identification and handling of other agency-originated information and FGI; (2) the threat of foreign intelligence activities attempting to obtain classified information; (3) the techniques employed by foreign intelligence activities to gain information; (4) insider threat; (5) the penalties for engaging in espionage; and (6) concerns identified during agency self-inspections.

ORIGINAL CLASSIFICATION AUTHORITY TRAINING

OCA's 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

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

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. Original classification authorities 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. OCA's sign an acknowledgement at the completion of the training session.

DERIVATIVE CLASSIFIER TRAINING

Persons who may apply derivative classification markings, regardless of media, receive training and are 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 (2) 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.

TERMINATION BRIEFINGS

Individuals receive termination briefings to inform them of their continuing security responsibilities after their access authorizations are terminated. A termination briefing is accomplished 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 Supervisor, personnel from the Personnel Security Division, or other personnel designated by Component management and the acknowledgement statement becomes part of the individual's permanent personnel security file.

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 receive more detailed additional training no later than six (six) months after assumption of duties that require this specialized training.

- A. Training topics may include, but are not limited to: overview of HUD safeguards and security disciplines, including personnel security, information security, physical security local access control procedures and escort requirements, protection of government property, locks and containers, risk management reporting and notification requirements, legal and administrative sanctions imposed for incurring a security infraction or committing a violation, construction security, SCIF construction, and/or foreign intelligence service threats to sensitive and classified information.
- B. SETA programs disseminate information concerning the following:

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

1. Applicable HUD safeguards and security directives and procedures;
2. Site specific (and/or operations-specific) safeguards and security policy, procedures, and requirements;
3. Other matters relating to security, including but not limited to, recent espionage cases, approaches, and recruitment techniques employed by foreign intelligence; and
4. Safeguards or security threats and vulnerabilities.

DOCUMENTATION REQUIREMENTS

Records are maintained to identify all individuals who have received briefings by type and date of briefing. Recordkeeping systems provide an audit trail. Statistics pertaining to total population and numbers that have received security briefings are maintained by each component and provided to the CISO when requested.

CHAPTER 9: SECURITY COMPLIANCE REVIEW PROGRAM

GENERAL

- A. The SCR program is the formal means by which HUD Components are measured to ensure efficient and effective management, implementation and oversight of HUD security programs and adequate security practices are in place for the protection of HUD personnel, property, information, and resources.
- B. Nothing in this Policy limits the authority of Component Heads to establish and implement Component specific SCR programs to cover their applicable Component activities. Component heads are encouraged to establish such programs in order to supplement and support the HUD CISO.
- C. The CISO SCR program is administered and managed by CISO.
- D. Nothing in this Policy limits the authority or interferes with the prerogatives of OIG as prescribed by the Inspector General Act of 1978, as amended.

ANNOUNCEMENTS AND CONDUCT

- A. Each Component is subject to an all-inclusive SCR at least once every three years. An all-inclusive SCR includes administrative security, physical security, personnel security, training, and OPSEC. SCRs or inspections conducted by an outside entity of a specific security discipline, such as the OPM for Personnel Security and the Information Security Oversight Office for Administrative Security, may substitute for the three (3)-year review of an applicable discipline when approved by HUD CISO.
- B. Each Component is subject to a SCR of their administrative security functions at least once every two (2) years. A review conducted in conjunction with the three (3)-year review schedule cited above serves as a two (2)-year review.
- C. To the extent practicable, and prior to scheduling an announced SCR the CISO coordinates with the recipient Component in order to ensure availability and to minimize any potential interference with other priority activities.
- D. Non-Federal officials and entities with which HUD shares classified information are subjected to a SCR of their administrative security functions on a schedule determined by HUD CISO.
- E. An off-schedule announced or unannounced SCR may be conducted of individual or multiple security disciplines as cited previously at the discretion of HUD CISO. Such reviews may also be conducted at the request of a Component head or designee.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

SELF-INSPECTION PROGRAMS

Each component that generates classified information is required to establish a self-inspection that includes regular reviews of a representative sample of its original and derivative classification actions.

- A. The self-inspection program reviews the following for adherence to the principles of EO 13526, 32 CFR 2001 and 2003, this Policy, and any component specific directives regarding: original classification, derivative classification, declassification, safeguarding, security violations, security education and training, management and oversight.
- B. Reviews include a representative sample of the component's derivatively classified products, to include electronic materials (e.g., email and presentations).
- C. The frequency of the self-inspections is determined by the needs of the component and the volume of classified material produced, but not less than annually.
- D. Checklists for self-inspections are maintained by CISO.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CHAPTER 10: INDUSTRIAL SECURITY PROGRAM

GENERAL

Participation in the NISP allows HUD to use the DSS to conduct investigations for contractor facility and personnel security clearances, and to monitor the contractor's compliance with safeguarding requirements. All facility and personnel security clearances granted by DOD are accepted by HUD as establishing eligibility for access to classified information. Contractors granted an interim facility and personnel clearance, such as an interim top secret, are eligible only for access to HUD classified information at the Secret level. Upon completion by DSS of all investigative requirements, that facility is considered eligible for access to classified information or award at the appropriate level granted by DSS.

DSS issues and maintains facility security clearances and personnel security clearances, as required, for HUD contractors. DSS inspects and monitors contractors that require or will require access to classified information. The DISCO, a field element of DSS, issues personnel security clearances under the authority of the NISP.

NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM)

The NISPOM (DOD 5220.22M) gives practical application to the objectives of the NISP (EO 12829) by serving as the single regulatory standard for the NISP. The NISPOM prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to contractors, in accordance with the NISP. The NISPOM also prescribes requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including RD, FRD, intelligence sources and methods information, SCI, and SAP information.

PROGRAM MANAGEMENT

Department and component programs, projects, and contracting personnel consider security requirements at the earliest possible stage in the procurement process. The responsibility for effective implementation of the Department's Industrial Security Program is shared by the project manager, contracting officer's technical representative/contracting officer's representative, security officials, and the contracting officer.

A. Security Clearances

To ensure that classified information entrusted to private industry is properly safeguarded, the Department requires that contractors requiring access to classified information in the completion of their contractual responsibilities be processed for security clearances in accordance with the requirements stipulated in the NISPOM.

B. Facility Security Clearance (FCL)

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

1. Any firm or business under contract with the Department that requires access to classified information requires a facility security clearance commensurate with the level of access required. Additionally, any firm or business entity that requires access to classified information to prepare a response to a Request for Proposal, Request for Bid, etc., and/or in performance of a classified Department contract requires a facility clearance.
2. Firms that do not possess a facility clearance, or the requisite level facility clearance, are sponsored for a DOD facility clearance when a determination has been made by the government contracting officer that the contract effort requires access to classified information. Facility clearance sponsorship requests are made by CISO to the DSS.
3. Facility clearances for sub-contracts are sponsored and processed by the prime contract in accordance with the NISPOM. These clearances are coordinated through the GCA, the contracting officer, and the Program Manager prior to submission.
4. If access is required for classified information, the request is be submitted to CISO for concurrence.
5. CISO maintains a copy of all DD254s.

C. Contractor Personnel

1. Individuals employed by a contractor are cleared through DISCO. The cleared contractor is required to have a designated FSO through which requests for personnel security clearances are submitted to DISCO. The FSO provides the appropriate HUD security office and contracting office with an updated status report of security clearance actions requested, pending, and approved. The FSO is also responsible for submitting visitor authorization requests on all cleared employees. Contractor personnel have clearances commensurate with the level of access required for performance under the contract. HUD has no role in the processing or granting of security clearances to industry personnel.

D. Contract Security Classification Specification (DD Form 254)

1. In order to activate DSS services and obligate the contractor to the provisions of the NISPOM, a *Contract Security Classification Specification* (DD Form 254) is included in all classified contracts and classified contract solicitations. The DD Form 254 is the primary vehicle for relating contract specific security classification guidance to the contractor and therefore, in Section 13 of the form, prescribes the source(s) from which the contractor derives security classification requirements. The source(s) either identify a published Security Classification Guide(s) applicable to the contract effort, or base that classification on existing classified information from which the contractor derives and applies classification guidance. Where the source(s) is identified as a security classification guide(s) the contractor is provided access to, or a copy of, the applicable guide(s).

FOR OFFICIAL USE ONLY (FOUO)

2. A DD Form 254 is required and completed only for contracts that require access to classified information.
3. Components that have an established Industrial Security Program prepare and process a DD Form 254 for each classified contract. A copy of all completed DD Forms 254 is submitted to the CISO.
4. Components that do not have an established Industrial Security Program coordinate preparation of the DD Form 254 with CISO. The statement of work or other documentation used to describe the services or supplies that are provided by the contract are provided to CISO to assist in preparation of the DD Form 254.
5. The contract, statement of work, or other documentation contains a security clause that a government contracting officer made a determination that the contract issued requires access to classified information by the contractor or his or her employees in the performance of the contract. This requirement is prescribed for all HUD classified contracts and applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post contract activity, or other GCA Programs which require access to classified information by a contractor.
6. In those cases where CISO prepares the DD Form 254, it returns the approved DD Form 254 to the component for inclusion in the contract or solicitation. CISO distributes a copy of the DD Form 254 to DSS, the contractor, and other components as applicable. DSS conducts investigations and issues the personnel security clearance(s) for the contract employees. With the exception of “carve out” contracts requiring access to Sensitive Compartmented Information or other SAPs, DSS provides security oversight functions in coordination with the CSO. CISO provides oversight for contracts involving access to SCI and SAP information.
7. In some instances, it may be necessary to include classified information in a DD Form 254 and facility clearance request. In these matters, the documentation is protected in a manner approved for classified information.

E. Classified Visits

1. Visit Requests

Components are to accept visit authorization letters only when the letters are submitted in accordance with and contain the information required by Chapter 6 of the NISPOM.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

2. Approvals

- a. All classified visits by contractors require advance notification to the component hosting the visit.
- b. Components only accept visit requests in writing. The visit authorization letter may be submitted either by email, mail, facsimile, or teletype, in sufficient time to allow for approval or disapproval of the requested visit. Telephonic verification of a visit request is not accepted except under exceptionally unique circumstances where: the failure to provide immediate access will have an adverse impact on the mission; unusual circumstances prevent the receipt or transmission of a written visit request as specified above; there is a means to authenticate the validity of the telephone request; and, acceptance of telephonic verification is approved by program management personnel. Instances not meeting these criteria result in a delay or denial of access until such time as a written request is received. Where telephonic verification is approved, written confirmation immediately follows.
- c. Hand-carried visit requests are not accepted.
- d. The component having security cognizance has final approval authority for the proposed visit. Components need not notify a requester that a visit has been approved if sufficient advance notice of the visit was provided. If the Component disapproves a visit, the requester is promptly notified.
- e. The number of classified visits is held to a minimum. The component determines the visit is necessary and requires access to classified information in order to approve a classified visit.

3. Precautions

- a. Components ensure visitors do not 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 host component or as otherwise specified in a classified contract.
- b. Components ensure that access to classified information at a level higher than the level of the visitor's clearance, certified in the visit authorization letter, is not granted. Access is not granted if the level of classified information exceeds the level required by a contract or specific purpose identified in the visit authorization letter.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

4. International Security Requirements

- a. ISAs with foreign governments address security controls, protection, and assurances 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 are in accordance with Chapter 10 of the NISPOM.
- b. At HUD, CISO oversees and administers the administration and oversight of classified exports, permanent and temporary imports of classified information, and compliance by cleared U.S. Contractors involved with NATO, foreign governments, and foreign contractors.
- c. CISO is responsible for maintaining a record of cleared U.S. contractors involved with foreign entities and related activities. Any disclosure or transfer of technical data to a foreign national is considered an “export,” regardless of where the transfer takes place. Components and contractors desiring to enter into international agreements, such as: Visits, Assignments, and Exchanges with Foreign Nationals, report these intentions to CISO. The report contains:
 - i. Name of Country
 - ii. Name and address of government entity issuing contract.
 - iii. Contract/RFP number.
 - iv. Name of U.S. contractor/name of any subcontractors involved.
 - v. Contract/RFP issue and response date.

Contractors are still required to report their activities to DSS per the NISPOM. CISO uses the report received from contractors to issue proper guidance to the component and to contractors to ensure compliance with governing export control laws before executing any agreement with a foreign interest that involves access to HUD-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 DOS and release of the classified information is subject to HUD approval. Failure to comply with Federal licensing requirements may render a contractor ineligible for a facility clearance.

FOR OFFICIAL USE ONLY (FOUO)

CHAPTER 11: ADMINISTRATIVE SECURITY REPORTING REQUIREMENTS

REPORTING OF ORIGINAL CLASSIFICATION AUTHORITIES

As required by EO 13526, HUD submits to CISO, a comprehensive list of all OCAs in the Department. This report is done on an annual basis or as required.

REPORTING OF SECURITY COMPLIANCE REVIEW ACTIVITIES

A summary of all security self-inspection activities is provided to CISO by September 30 of every year in a format determined by CISO. Further, CISO reports such activities to the OCAO SSO pursuant to EO 13526.

FUNDAMENTAL SECURITY CLASSIFICATION GUIDE REVIEW

No later than July 1, OSCO, with the assistance of the affected Components, reviews and updates all existing classification guides. In addition to incorporating changes consistent with EO 13526, the review certifies the validity of all classification decisions incorporated into the guides. A summary of the review is sent to the OCAO SSO. Additionally, a version suitable for public release is also generated.

CLASSIFICATION COST REPORTING

- A. As required by EO 13526, HUD submits to the OCAO SSO, via CISO, an estimate of the costs associated with classification activities at the Department. The report combines the input received from all HUD Components into a single HUD report. This report is required on an annual basis.
- B. Components collect the required information for the Component's respective areas based on guidance provided by CISO.

CLASSIFICATION ACTIVITY REPORT (311 REPORTING)

- A. As required by EO 13526, HUD submits to the OCAO SSO, via the CISO, an annual report reflecting the degree of classification activity occurring within the Department for the preceding fiscal year. The report is completed using the SF 311, *Agency Security Classification Management Program Data*, and combines the input of all HUD Components into a single HUD report.
- B. Components collect the required information for the Component's respective areas based on guidance provided by CISO.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

CHAPTER 12: STANDARD FORMS

GENERAL

The purpose of the standard forms is to promote the implementation of the government-wide IASP. Standard forms are prescribed when the use enhances the protection of national security information and/or reduces the costs associated with its protection. The use of the standard forms prescribed is mandatory for agencies of the executive branch that create or handle national security information.

AVAILABILITY

Offices may obtain copies of the standard forms prescribed by ordering through the GSA Consumer Global Supply Centers, or the GSA Advantage on-line service. Some of these standard forms can be downloaded from the GSA Forms Library.

STANDARD FORMS

Standard forms required for application to national security information are as follows:

A. SF 311, *Agency Security Classification Management Program Data*

The SF 311 is a data collection form completed by only those Executive Branch agencies that create and/or handle classified national security information. The form is a record of classification management data provided by the agencies. The agencies submit the completed forms on an annual basis to the OCAO SSO, no later than November 15 following the reporting period, for inclusion in a report to the President.

B. SF 312, *Classified Information Nondisclosure Agreement*:

1. The SF 312 is a nondisclosure agreement between the United States and an employee of the Federal Government or one of its contractors, licensees, or grantees. With the exception of an emergency as defined in section 4.2(b) of EO 13256, this form is executed prior to the grant of classified information by the United States Government.
2. Electronic (digital) signatures and signature stamps on SF 312s are prohibited.
3. The SF 312 is the current authorized form; if an employee originally signed the now outdated SF 189 or SF 189-A, or a form under an approved waiver as agreement to nondisclosure, the forms remain valid. The SF 189 and SF 189-A are no longer available for use with new employees.
4. The use of the "Security Debriefing Acknowledgement" portion of the SF 312 is optional. If a component chooses not to record its debriefing by signing/dating the debriefing section of the SF 312, then the component provides an alternative record.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

5. An authorized representative of a contractor, licensee, grantee, or other non-Government organization, acting as a designated agent of the United States, may witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States. Also, an employee of a United States agency may witness the execution of the SF 312 by an employee, contractor, licensee, or grantee of another United States agency, provided that an authorized United States Government official or, for non-Government employees only, a designated agent of the United States subsequently accepts by signature the SF 312 on behalf of the United States.
6. The provisions of the SF 312, the SF 189, and the SF 189–A do not supersede the provisions of 5 U.S.C. 2302, which pertain to the protected disclosure of information by Government employees, or any other laws of the United States.
7. Each agency retains its executed copies of the SF 312, SF 189, and SF 189–A in file systems from which an agreement can be expeditiously retrieved in the event that the United States seeks its enforcement or a subsequent employer needs to confirm its prior execution. The original, or a legally enforceable facsimile that is retained in lieu of the original, such as microfiche, microfilm, computer disk, or electronic storage medium, is retained for 50 years following its date of execution. For agreements executed by civilian employees of the United States Government, an agency may store the executed copy of the SF 312 and SF 189 in the United States OPM’s Official Personnel Folder as a long-term (right side) document for that employee. An agency may permit its contractors, licensees, and grantees to retain the executed agreements of their employees during the time of employment. Upon the termination of employment, the contractors, licensee, or grantee delivers the original or legally enforceable facsimile of the executed SF 312, SF 189 or SF 189–A of that employee to the Government agency primarily responsible for his or her classified work. A contractor, licensee, or grantee of an agency participating in the NISP provides the copy or legally enforceable facsimile of the executed SF 312, SF 189 or SF 189–A of a terminated employee to the cognizant security office. Internally, HUD informs the OCAO SSO of the file systems that it uses to store these agreements for each category of affected individuals.
8. The national stock number for the SF 312 is 7540–01–280–5499.

C. SF 700, Security Container Information

The SF 700 provides the names, addresses, and telephone numbers of employees who are to be contacted if the security container to which the form pertains is found open and unattended. The form also includes the means to maintain a current record of the security container's combination and provides the envelope to be used to forward this information to the appropriate component official. Parts 2 and 2A of each completed copy of SF 700 are classified at the highest level of classification of the information authorized for storage in the security container. A new SF 700 is completed each time the combination to the security container is changed. The national stock number for the SF 700 is 7540–01–214–5372.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

D. SF 701, *Activity Security Checklist*

The SF 701 provides a systematic means to make a thorough end-of-day security inspection for a particular work area and to allow for employee accountability in the event that irregularities are discovered. If a Component determines, as part of its risk management strategy, that an activity security checklist is required, the SF 701 is used. Completion, storage, and disposition of SF 701 is in accordance with each Component's security requirements. The national stock number for the SF 701 is 7540-01-213-7899.

E. SF 702, *Security Container Check Sheet*

The SF 702 provides a record of the names and times that persons have opened, closed, or checked a particular container that holds classified information. The national stock number of the SF 702 is 7540-01-213-7900.

F. SF 703, TOP SECRET Cover Sheet

The SF 703 serves as a shield to protect TOP SECRET classified information from inadvertent disclosure and to alert observers that TOP SECRET information is attached to it. The SF 703 is affixed to the top of the TOP SECRET document and remains attached until the document is downgraded, requiring the appropriate classification level cover sheet, declassified, or destroyed. When the SF 703 has been appropriately removed, it may, depending upon its condition, be reused. The national stock number of the SF 703 is 7540-01-213-7901.

G. SF 704, *SECRET Cover Sheet*

The SF 704 serves as a shield to protect SECRET classified information from inadvertent disclosure and to alert observers that SECRET information is attached to it. The SF 704 is affixed to the top of the SECRET document and remains attached until the document is downgraded, requiring the appropriate classification level cover sheet, declassified, or destroyed. When the SF 704 has been appropriately removed, it may, depending upon its condition, be reused. The national stock number of the SF 704 is 7540-01-213-7902.

H. SF 705, *CONFIDENTIAL Cover Sheet*

The SF 705 serves as a shield to protect CONFIDENTIAL classified information from inadvertent disclosure and to alert observers that CONFIDENTIAL information is attached to it. The SF 705 is affixed to the top of the CONFIDENTIAL document and remains attached until the document is destroyed. When the SF 705 has been appropriately removed, it may, depending upon its condition, be reused. The national stock number of the SF 705 is 7540-01-213-7903.

I. SF 706, *TOP SECRET Label*

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

The SF 706 is used to identify and protect electronic media and other media that contain TOP SECRET information. The SF 706 is used instead of the SF 703 for media other than documents. The SF 706 is affixed to the medium containing TOP SECRET information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 706 is 7540-01-207-5536.

J. SF 707, SECRET Label

The SF 707 is used to identify and protect electronic media and other media that contain SECRET information. The SF 707 is used instead of the SF 704 for media other than documents. The SF 707 is affixed to the medium containing SECRET information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 707 is 7540-01-207-5537.

K. SF 708, CONFIDENTIAL Label

The SF 708 is used to identify and protect electronic media and other media that contain CONFIDENTIAL information. The SF 708 is used instead of the SF 705 for media other than documents. The SF 708 is affixed to the medium containing CONFIDENTIAL information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 708 is 7540-01-207-5538.

L. SF 709, CLASSIFIED Label

The SF 709 is used to identify and protect electronic media and other media that contain classified information pending a determination by the classifier of the specific classification level of the information. The SF 709 is affixed to the medium containing classified information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. When a classifier has made a determination of the specific level of classification of the information contained on the medium, either the SF 706, SF 707, or SF 708 is affixed on top of the SF 709 so that only the SF 706, SF 707, or SF 708 is visible. The national stock number of the SF 709 is 7540-01-207-5540.

M. SF 710, UNCLASSIFIED Label

In a mixed environment in which classified and unclassified information are being processed or stored, the SF 710 is used to identify electronic media and other media that contain unclassified information. Its function is to aid in distinguishing among those media that contain either classified or unclassified information in a mixed environment. The SF 710 is affixed to the medium containing unclassified information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. However, the label is small enough so that it can be wholly covered by a SF 706, SF 707, SF 708, or SF 709 if the medium

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

subsequently contains classified information. The national stock number of the SF 710 is 7540–01–207–5539.

N. SF 711, DATA DESCRIPTOR Label

The SF 711 is used to identify additional safeguarding controls that pertain to classified information that is stored or contained on electronic or other media. The SF 711 is affixed to the electronic medium containing classified information in a manner that would not adversely affect operation of equipment in which the medium is used. The SF 711 is ordinarily used in conjunction with the SF 706, SF 707, SF 708, or SF 709, as appropriate. Once the label has been applied, it cannot be removed. The SF 711 provides spaces for information that should be completed as required. The national stock number of the SF 711 is 7540–01–207–5541.

O. SF 714, Financial Disclosure Report

When required, the SF 714 contains information that is used to make personnel security determinations, including whether to grant a security clearance; to allow access to classified information, sensitive areas, and equipment; or to permit assignment to sensitive national security positions. The data may later be used as a part of a review process to evaluate continued eligibility for access to classified information or as evidence in legal proceedings. The SF 714 assists law enforcement agencies in obtaining pertinent information in the preliminary stages of potential espionage and counter terrorism cases.

P. SF 715, Government Declassification Review Tab

The SF 715 is used to record the status of classified national security information reviewed for declassification. The SF 715 is used in all situations that call for the use of a tab as part of the processing of records determined to be of permanent historical value. The national stock number for the SF 715 is 7540-01-537-4689.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

APPENDIX A: DEFINITIONS

1. Access: means the ability or opportunity to gain knowledge of classified information.
2. Accessioned records: means records of permanent historical value in the legal custody of NARA.
3. Agency: means any “Executive agency,” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.
4. Authorized holder: of classified information means anyone who satisfies the conditions for access stated in EO 13526.
5. Authorized person: means a person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know.
6. Automated information system: means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.
7. Automatic declassification: means the declassification of information based solely upon:
 - a. the occurrence of a specific date or event as determined by the original classification authority; or
 - b. the expiration of a maximum time frame for duration of classification established under E.O. 13526.
8. Classification: means the act or process by which information is determined to be classified information.
9. Classification guidance: means any instruction or source that prescribes the classification of specific information.
10. Classification guide: means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.
11. Classification management: means the life-cycle management of classified national security information from original classification to declassification.
12. Classified document: any recorded classified information, regardless of its physical/electronic form or characteristics, including, without limitation, written or printed matter, tapes, charts, maps, paintings, drawings, engravings, sketches, working notes and papers; reproductions of such things by any means of process; and sound, voice, magnetic, or electronic recordings in any form.
13. “Classified national security information” or “classified information”: means information that has been determined pursuant to EO 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

FOR OFFICIAL USE ONLY (FOUO)

14. Classified spillage: the accidental, inadvertent, or intentional introduction of classified information into an unclassified information technology system or higher-level classified information into lower level classified information technology system, to include non-government systems.
15. Cleared commercial carrier: means a carrier that is authorized by law, regulatory body, or regulation, to transport Secret and Confidential material and has been granted a Secret facility clearance in accordance with the National Industrial Security Program.
16. Compilation: means an aggregation of preexisting unclassified items of information, the association of which classifies the whole.
17. Component Chief Security Officer (CCSO): the senior-most Federal security executive designated by the Head of the Component in the following Components: U.S. Coast Guard; U.S. Secret Service; U.S. Customs and Border Protection; U.S. Immigration and Customs Enforcement; Transportation Security Administration; U.S. Citizenship and Immigration Services; Federal Emergency Management Agency; and Federal Law Enforcement Training Center.
18. Compromise: any occurrence that results or may likely result in unauthorized persons gaining access to classified information.
19. COMSEC: the communications security systems, services, and concepts that constitute protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of any/such communications.
20. Confidential: level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
21. Confidential source: means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.
22. Control: means the authority of the agency that originates information, or its successor in function, to regulate access to the information.
23. Damage to the national security: means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.
24. Damage Assessment: systemic analysis that determines the impact of a compromise of classified information on the national security of the United States.
25. Declassification: means the authorized change in the status of information from classified information to unclassified information.

FOR OFFICIAL USE ONLY (FOUO)

26. Declassification authority: the official who authorized the original classification, if that official is still serving in the same position; the originator's current successor in function; a supervisory official of either; or officials delegated declassification authority in writing by the agency head or senior agency official.
27. Declassification guide: means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.
28. Derivative classification: means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.
29. Document: means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.
30. Downgrading: means a determination by a declassification authority that information classified and safeguarded at a specified level is classified and safeguarded at a lower level.
31. Employee: means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal service contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.
32. Equity: refers to information;
 - a. Originally classified by or under the control of an agency;
 - b. In the possession of the receiving agency in the event of transfer of function; or
 - c. In the possession of a successor agency for an agency that has ceased to exist.
33. Exempted: means nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification under EO 13526.
34. Facility: means an activity of an agency authorized by appropriate authority to conduct classified operations or to perform classified work.
35. Federal records: includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal Law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in the materials. Library and museum material made or acquired and preserved solely for reference, and stocks of publication and processed documents are not included. (44 U.S.C. 3301)

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

36. File series: means file units or documents arranged according to a filing system or kept together because the units or documents relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.
37. Foreign government information: means:
- a. information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
 - b. information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
 - c. information received and treated as “foreign government information” under the terms of a predecessor order.
38. For Official Use Only (FOUO): means the term used within HUD to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States is classified Confidential, Secret, or Top Secret under EO 13526, or its predecessor or successor orders, and is not considered to be FOUO. FOUO is not considered to be classified information.
39. Freedom of Information Act (FOIA): provides that any person has a right of access to federal agency records, except to the extent that such records are protected from public disclosure by statutory exemption or exclusions.
40. Information: means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by, is produced by or for, or is under the control of the United States Government.
41. Information security: means the system of policies, procedures, and requirements established under the authority of EO 13526, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.
42. Infraction: means any knowing, willful, or negligent action contrary to the requirements of EO 13526 or its implementing directives that does not constitute a “violation,” as defined below.
43. Integral file block: means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks contain only records dated within 10 years of the oldest record in the file block.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

- 44. Integrity: means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.
- 45. Intelligence: includes foreign intelligence and counterintelligence as defined by EO 12333, December 4, 1981, as amended, or by a successor order.
- 46. Intelligence activities: means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or EO 12333, as amended, or a successor order.
- 47. Intelligence Community: means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of EO 12333, as amended.
- 48. Mandatory declassification review: means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of EO 13526.
- 49. Multiple sources: means two or more source documents, classification guides, or a combination of both.
- 50. National security: means the national defense or foreign relations of the United States.
- 51. Need-to-know: means a determination within the executive branch in accordance with directives issued pursuant to EO 13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
- 52. Network: means a system of two or more computers that can exchange data or information.
- 53. Newly discovered records: means records that were inadvertently not reviewed prior to the effective date of automatic declassification because the appropriate agency personnel were unaware of the existence of the records.
- 54. Open storage area: means an area constructed in accordance with §2001.53 of 32 CFR parts 2001 and 2003 and authorized by the agency head for open storage of classified information.
- 55. Original classification: means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.
- 56. Original classification authority with jurisdiction over the information: includes;
 - a. The official who authorized the original classification, if that official is still serving in the same position;
 - b. The originator's current successor in function;
 - c. A supervisory official of either; or
 - d. The senior agency official under EO 13526
- 57. Original classification authority: means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

58. Permanent records: means any Federal record that has been determined by the National Archives to have sufficient value to warrant its preservation in the National Archives. Permanent records include all records accessioned by the National Archives into the National Archives and later increments of the same records, and those for which the disposition is permanent of SF 115s, Request for Records Disposition Authority, approved by the National Archives on or after May 14, 1973.
59. Permanently valuable information or permanent historical value: refers to information contained in:
- a. Records that have been accessioned by the National Archives;
 - b. Records that have been scheduled as permanent under a records disposition schedule approved by the National Archives; and
 - c. Presidential historical materials, presidential record or donated historical materials located in the National Archives, a presidential library, or any other approved repository.
60. Presidential papers, historical materials, and records: means the papers or records of the former Presidents under the legal control of the Archivist pursuant to section 2111, 2111 note, or 2203 of title 44, U.S.C. Protected Critical Infrastructure Information (PCII): critical infrastructure information (CII) defined in 6 U.S.C 671 (3) (Section 213 (3) of the Homeland Security Act). Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.
61. Records: means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.
62. Records having permanent historical value: means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.
63. Records management: means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.
64. Redaction: means the removal of classified information from copies of a document such that recovery of the information on the copy is not possible using any reasonably known techniques or analysis.
65. Risk management principles: means the principles applied for assessing threats and vulnerabilities and implementing security countermeasures while maximizing the sharing of information to achieve an acceptable level of risk at an acceptable cost.
66. Safeguarding: means measures and controls that are prescribed to protect classified information.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

67. Secret: level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
68. 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 Intrusion Detection System (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.
69. Security Liaison: means an official who is assigned responsibility for implementation and management of a Component's security programs as a secondary or additional duty.
70. Security Officer: means an authorized position within a Component, the primary duties of which are to serve as the lead official for the development, implementation, and management of security programs within the Component.
71. Self-inspection: means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under EO 13526 and its implementing directives.
72. Senior agency official: means the official designated by the agency head under section 5.4(d) of EO 13526 to direct and administer the agency's program under which information is classified, safeguarded, and declassified.
73. Sensitive Security Information (SSI): Sensitive Security information (SSI) is defined in 49 CFR part 1520. SSI is a specific category of information that requires protection against disclosure.
74. Source document: means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.
75. Special access program: means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.
76. Supplemental controls: means prescribed procedures of systems that provide security control measures designed to augment the physical protection of classified information. Examples of supplemental controls include intrusion detection systems, periodic inspections of security containers or areas, and security-in-depth.
77. Systematic declassification review: means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.
78. Telecommunications: means the preparation, transmission, or communication of information by electronic means.

FOR OFFICIAL USE ONLY (FOUO)

79. Temporary records: means Federal records approved by NARA for disposal, either immediately or after a specified retention period. Also called disposable records.
80. Top Secret: level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
81. Transclassification: means information that has been removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, and safeguarded under applicable EOs as “National Security Information.”
82. Unauthorized disclosure: means a communication or physical transfer of classified information to an unauthorized recipient.
83. Unscheduled records: means Federal records which do not have a final disposition approved by NARA. All records that fall under a NARA approved records control schedule are considered to be scheduled records.
84. U.S. entity includes:
- a. State, local, or tribal governments;
 - b. State, local, and tribal law enforcement and firefighting entities;
 - c. public health and medical entities;
 - d. regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or
 - e. private sector entities serving as part of the nation’s Critical infrastructure/Key Resources.
85. Violation: means:
- 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 EO 13526 and its implementing directives; or
 - c. any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of EO 13526.

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM

APPENDIX B: FORMS

1. DHS Form 11000-2, *Courier Authorization Request*
2. SF 135-85b, *Records Transmittal And Receipt*
3. DHS Form 11000-11, *Record of Security Violation*

FOR OFFICIAL USE ONLY (FOUO)

INFORMATION AND ADMINISTRATIVE SECURITY PROGRAM