ADS Chapter 568

National Security Information Program

Full Revision Date: 05/19/2017
Responsible Office: SEC/CTIS
File Name: 568_051917

Functional Series 500 - Management Services Chapter 568 - National Security Information Program
POC for ADS 568: Diane Sloan, (202) 712-0894, dsloan@usaid.gov

***This chapter has been revised in its entirety*.**

Table of Contents

Chapter 568 - National Security Information Program

568.1 OVERVIEW

Effective Date: 05/19/2017

This ADS chapter provides the policy directives and required procedures for USAID's implementation of the Information Security Program, which includes classification of national security information, the storage and safeguarding of classified information, security education and awareness, the security incident program, as well as access, control, and dissemination.

The **Executive Order (EO) 13526, Classified National Security Information**; **EO 12968, Access to Classified Information**; **EO 13467 Roles and Responsibilities of the National Background Investigations Bureau and Related Matters**; **EO 12829, National Industrial Security Program**; **National Industrial Security Program Operating Manual (NISPOM)**; and **12 FAM 500, Information Security**.

Throughout this chapter, the term "workforce" or "members of the workforce" refers to individuals working for, or on behalf of, the Agency, regardless of hiring or contracting mechanism, whose job involves physical and/or logical access to USAID. This may include Direct-Hire employees, Personal Services Contractors, Participating Agency Service Agreement (PASAs) and contractor personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS 501.1**. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to HSPD-12 and Information Security requirements.

568.2 PRIMARY RESPONSIBILITIES

Effective Date: 05/19/2017

a. The **Administrator (A/AID)** has the authority to originally classify information and is responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

b. The **USAID Director of Security (D/SEC)** is the USAID senior Agency official under Executive Orders (EOs) 13526, 12968, and 13467. The responsibilities of the senior Agency official are stipulated in each of the EOs (see **EO 13526**, **EO 12968**, **EO 13467** and **EO 12829**).

c. The **Office of Security, Chief, Counterterrorism Information Security Division (SEC/CTIS)** is responsible for overseeing and implementing program policies and responsibilities related to the Information and Industrial Security (IIS) program. The Chief, CTIS maintains oversight of all USAID Sensitive Compartmented Information Facilities (SCIFs).

d. The **Executive Secretariat (ES)** of the Agency, who retains special security

representatives (SSRs) working under the direction of the Office of Security (SEC) Special Security Officer (SSO), is responsible for the day-to-day management of the Sixth Floor Sensitive Compartmented Information Facility.

e. The **Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD)** is responsible for administering the USAID program for systematic and mandatory declassification reviews of classified documents. These responsibilities include data collection and statistical analysis reporting and preparation of reports requested by the Information Security Oversight Office (ISOO).

f. The **Unit Security Officer (USO)** is responsible for ensuring that all operations within his or her respective Mission or Bureau/Independent Offices (B/IO) are carried out in accordance with the security regulations in this ADS chapter. This responsibility is generally delegated to the Executive Officer (EXO).

g. The **Administrative Management Specialist (AMS)** in each B/IO is responsible for coordination and documentation of classification activity, end-of-day security checks, training, and corrective actions related to security incidents or findings.

h. The **Original Classification Authority (OCA)** is responsible for the annual review of the USAID Classification Guide and the proper conduct and documentation of classification decisions.

i. The **Office of Human Capital and Talent Management, Employee Labor Relations (HCTM/ELR)** is responsible for coordinating with SEC for formal disciplinary actions for non-compliance with policies.

568.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

568.3.1 Classification of National Security Information

Effective Date: 05/19/2017

12 FAM 500 contains the policy and procedures for USAID and all foreign affairs agencies concerning the implementation of **EO 13526**. The policies and required procedures in this ADS chapter supplement **12 FAM 500** for USAID and must be considered in conjunction with **12 FAM 500** and **EO 13526**.

The head of each Bureau/Independent Office (B/IO) and overseas USAID Mission must appoint a Unit Security Officer (USO). Individuals with original classification authority; security managers or security specialists; and employees whose duties significantly involve the creation or handling of classified information, including employees who regularly apply derivative classification markings, will be evaluated for this activity during the annual performance period. This requirement also applies to USAID employees including, but not limited to, Executive Officers (EXOs), Administrative Management Specialists (AMSs), USOs, and employees within the Administrator's office (A/AID), the Executive Secretariat (ES), and the Office of Security (SEC). The evaluation will assess

their ability to designate and manage classified information and will be considered a critical element in the AEFs for all employees.

568.3.1.1 Classified Information Levels

Effective Date: 05/19/2017

Information is deemed classified when it is determined that the unauthorized disclosure of that information could cause some degree of damage to national security. Information may be classified at one of the following levels (see **EO 13526**):

- Confidential: must be 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.

- Secret: must be 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.

- Top Secret: must be 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.

Except as otherwise provided by statute, no other terms will be used to identify United States classified information.

If there is significant doubt about the appropriate level of classification, the authorized creator of the information must classify it at the lower level.

568.3.1.2 Original Classification Authority

Effective Date: 05/19/2017

"Original classification" means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

Information may be originally classified under the terms of **EO 13526** only if all of the following conditions are met:

- An original classification authority is classifying the information;

- The information is owned by, produced by or for, or is under the control of the United States Government;

- The information falls within one or more of the categories of information listed in section 1.4 of **EO 13526**; and

The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage. The unauthorized disclosure of foreign government information is presumed to cause damage to national security.

If the OCA has significant doubt about the need to classify information, it must not be classified.

Classified information will not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

As prescribed in **EO 13526**, the authority to classify information originally may be exercised only by the President, agency heads, officials designated by the President in the Federal Register, or other United States Government officials delegated this authority. Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

Delegation of original classification authority must be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

Each delegation of original classification authority must be in writing and the authority must not be re-delegated except as provided in this order.

The number of USAID officials possessing original classification authority as outlined in **EO 13526** is strictly limited. USAID officials do not have the authority to classify at the Top Secret (TS) or Sensitive Compartmented Information (SCI) level. As the Agency head, the Administrator (A/AID) has the authority to originally classify information at the Confidential and Secret level. Authority to originally classify at the Confidential and Secret level has been delegated by the Administrator to the following positions:

- Deputy Administrator (DA/AID),

- Inspector General (IG), and

- Director of Security (D/SEC).

In order to ensure the appropriateness of classifications, the respective AMS officials or special assistants for A/AID, DA/AID, D/SEC and IG must report the following information to SEC/CTIS/IIS no later than September 30 each year:

- All original classification decisions made by their respective Original Classification Authority (OCA) to include the classification level,
- Document type,
- Reason for classification,
- The OCA's name,
- Declassification date, and
- The date on which the document was classified.

If a member of the workforce has or believes they have information that should be originally classified, they must contact an OCA or reference a classification guide for further guidance. USAID employees within the continental U.S. should contact one of the OCAs listed above or reference USAID's Classification Guide (see **568.3.1.4**). The USAID workforce overseas should contact the Regional Security Officer or reference USAID's Classification Guide.

[Note: All members of the workforce with a valid security clearance and who complete the mandatory annual security refresher training possess derivative classification authority. These individuals may derivatively classify information in hard copy and electronic form. **EO 13526** states "persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority." **EO 13526, section 2.1** and the Information Security Oversight Office's booklet entitled **Marking Classified National Security Information (December 2010, Revision 3, August 2016)** outline the procedures for exercising derivative classification and marking of documents.]

568.3.1.3 Classification Challenges

Effective Date: 05/19/2017

As per **EO 13526**, section 1.8, authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information. If holders or recipients of classified information have substantial reason to believe that the information is improperly classified, they must communicate that belief to the classifier of the information. Individuals are not subject to retribution for bringing such actions. The classification authority block will identify the classifier of the information on the classified document as indicated in **568.3.1.7**

Members of the workforce challenging a classification must sufficiently describe the information being challenged to permit identification of the information and its classifier. Individuals challenging a classification must also include the reason(s) why the challenger believes that the information is classified improperly or unnecessarily.

These individuals may direct classification challenges, allegations, or complaints regarding over-classification or incorrect classification within the Agency in writing or electronically through the secure classified computer systems to an OCA. Individuals are provided with the opportunity for their challenge to be reviewed by an impartial official or panel. Individuals accessing the classified computer systems must have a security clearance, attend a mandatory training on how to properly use the system, and sign the appropriate user agreement.

OCAs receiving challenges pursuant to this section must provide a response within 30 calendar days of the confirmed receipt of the challenge. The OCA must notify the challenger of any changes made as a result of the challenge or the reasons why no change was made. Pending final determination of a challenge to classification, OCAs must safeguard the information or document in question as required for the level of classification initially assigned.

If not resolved by the OCA, the challenger may appeal the decision to SEC/CTIS. SEC/CTIS must provide a response within 30 calendar days of the confirmed receipt of the appeal. If resolution cannot be obtained within the Agency, further appeal may be made to the Interagency Security Classification Appeals Panel (ISCAP). The timeframe in which ISCAP will respond to appeals is solely determined by ISCAP. Documents required to be submitted for prepublication review or other administrative process pursuant to an approved non-disclosure agreement are not covered by **EO 13526**, section 1.8.

568.3.1.4 Classification Guide

Effective Date: 05/19/2017

The USAID workforce can use USAID's Classification Guide to derivatively classify information. As per **EO 13526** and **32 CFR Parts 2001 and 2003**, an individual is determined to have derivative classification authority if they have the appropriate security clearance and have completed derivative classification training every year.

USAID's Classification Guide may be used by those who have derivative classification authority to assist in avoiding over-classification. It is imperative that classified information is properly marked and classified at the appropriate level to protect national security. USAID's Classification Guide is classified and available through the secure classified computer systems.

568.3.1.5 Fundamental Classification Guidance Review (FCGR)

Effective Date: 05/19/2017

As per **EO 13526** and **32 CFR Parts 2001 and 2003**, SEC must complete, on a periodic basis, a comprehensive review of the Agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified.

As per **32 CFR Part 2001**, USAID will conduct a fundamental classification guidance review at least once every five years. 32 CFR Part 2001.16 explains the items that should be focused on throughout the review. A detailed report summarizing the results of each classification guidance review is provided by the IIS Branch to the Information Security Oversight Office (ISOO).

The classification guidance review includes an evaluation of classified information to determine if it meets the standards for classification under section 1.4 of **EO 13526**, taking into account an up-to-date assessment of likely damage as described under section 1.2 of **EO 13526**. The goal of the Fundamental Classification Guidance Review (FCGR) is to ensure agency classification guidance authorizes classification only in those specific instances necessary to protect national security. ISOO provides guidance on completing the FCGR to the Senior Agency Official.

The classification guidance review includes original classification authorities and agency subject matter experts to ensure a broad range of perspectives. The head of each B/IO and the OCA must conduct an annual review of the USAID Classification Guide (a copy of the Guide may be obtained by contacting SEC/CTIS/IIS at **secinformationsecurity@usaid.gov**) and submit any recommended changes in writing to SEC/CTIS. The designated B/IO reviewer or OCA may recommend the addition of specific types of information to be classified or the modification of specific portions of the Guide, as applicable, to meet the program requirements of their respective B/IO.

SEC reports its classification guidance reviews to the Director of the Information Security Oversight Office (ISOO).

568.3.1.6 Annual Summary Preparation, SF-311 Report

Effective Date: 05/19/2017

The Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD) will prepare an annual summary of all documents reviewed and declassified during the fiscal year. M/MS/IRD must provide the summary to the Office of Security (SEC) at the conclusion of each fiscal year for inclusion in the Agency's annual report to the ISOO. This report is due to ISOO by November of each year.

SEC will coordinate and collaborate with the AMS/USO in B/IOs, as appropriate, to collect a representative sample of classification actions (derivative and original) performed by authorized classifiers based upon ISOO guidance and methodologies for the **SF-311, Agency Security Classification Management Program Data** form.

SEC hosts an annual face-to-face SF-311 sampling training for AMS/USOs. Each B/IO must send a representative to participate in the training. The AMS/USO representative must communicate the information provided in the training to the entire B/IO. In the training, the AMS/USO will be provided with the SF-311, Survey Sheet and receive training on how to properly fill it out and submit to SEC. AMS/USOs will also receive training on the sampling methodology, approved by ISOO, to arrive at the total classification decision numbers for the entire year. SEC will determine the sampling population and sampling period and communicate this to the AMS/USO at this training. Members of the workforce must provide their AMS/USO with their classification numbers so the AMS/USO can complete and submit the SF-311, Survey Sheet to SEC no later than October 15 or by the date provided at the sampling training (whichever occurs first for that calendar year), each year for inclusion in the Agency's annual report to the ISOO. Individuals must also report negative responses (i.e. if an individual has no classification decisions). For questions on this report and its requirements, contact the IIS branch at **secinformationsecurity@usaid.gov**.

See ISOO's Web site, **https://www.archives.gov/isoo template**, for the SF-311 template and FAQs.

568.3.1.7 Identification and Marking

Effective Date: 05/19/2017

All members of the workforce must identify and mark all classified material as provided in section 1.6 of **EO 13526**. Paper document markings must not deviate from the format prescribed in **EO 13526** and the Information Security Oversight Office's booklet entitled **Marking Classified National Security Information (December 2010, Revision 3, August 2016)**. This booklet addresses various topics related to markings, including but not limited to:

- Original and derivative classification decisions,
- Additional or special markings,
- Foreign government information,
- Declassification instructions,
- Portion markings,
- The identity of the classification authority and office of origin, and
- The date or event for declassification.

568.3.1.8 Classification Prohibitions and Limitations

Effective Date: 05/19/2017

In no case will information be classified, maintained as classified, or fail to be declassified in order to:

- Conceal violations of law, inefficiency, or administrative error;
- Prevent embarrassment to a person, organization, or agency;
- Restrain competition; or
- Prevent or delay the release of information that does not require protection in the interest of the national security.

Basic scientific research information not clearly related to the national security should not be classified. Information may not be reclassified after declassification and then released to the public under proper authority unless:

- The reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security;
- The information may be reasonably recovered without bringing undue attention to the information;
- The reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office; and
- For documents in the physical and legal custody of the National Archives and Records Administration (National Archives) that have been available for public use, the agency head has, after making the determinations required by this paragraph, notified the Archivist of the United States (Archivist), who must suspend public access pending approval of the reclassification action by the Director of the Information Security Oversight Office. Any such decision by the Director may be appealed by the agency head to the President through the National Security Advisor. Public access must remain suspended pending a prompt decision on the appeal.

Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the **Freedom of Information Act (5 USC 552)**, the **Presidential Records Act, 44 USC 2204(c)(1)**, the **Privacy Act of 1974 (5 USC 552a)**, or the mandatory review provisions of section 3.5 of Executive Order 13526 (only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the Agency head, the Deputy Agency head, or D/SEC). The requirements in this paragraph also apply to those situations in which

information has been declassified in accordance with a specific date or event determined by an original classification authority in accordance with section 1.5 of **EO 13526**.

Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information.

568.3.1.9 SEC Review

Effective Date: 05/19/2017

At SEC's request, B/IOs must make all classified documents and classified emails that originated within USAID available to SEC for review for compliance with marking and classification requirements. This review includes electronic copies of originally and derivatively classified documents.

In USAID/Washington (USAID/W), members of the workforce that derivatively or originally classify documents may be requested to complete an unclassified record reflecting the number of documents classified, if they were originally or derivatively classified, and the level of classification. This is not required to be noted throughout the year. This will be part of the SF-311 sampling referenced in **568.3.1.1**, prompted by the IIS Branch for the B/IO's AMS/USO to request from their workforce. This information will be reported by the IIS Branch to the ISOO.

568.3.1.10 FOIA Review

Effective Date: 05/19/2017

Recipients of Freedom of Information Act (FOIA) requests involving classified information must direct the requests in writing to SEC/CTIS/IIS and M/MS/IRD for review and concurrence.

SEC has the authority to exercise the national security exemption as stated in the **Freedom of Information Act, 5 USC 552b (1**) when responding to FOIA requests. SEC must verify that the information involved clearly meets the standards for continued classification regardless of the markings to include declassification instructions contained in the document. SEC will collaborate with M/MS/IRD regarding such requests.

568.3.2 Access, Control, and Dissemination

Effective Date: 05/19/2017

a. Approved custodians or users of classified information are personally responsible for the protection and control of this information. These individuals must safeguard classified information at all times to prevent loss or compromise and unauthorized

disclosure, dissemination, or duplication. Unauthorized disclosure of classified material is punishable under federal criminal statutes and local policies.

b. Persons in possession of classified information must not give access to the information to other persons unless such access is necessary for the performance of the recipient's official duties. In addition, the recipient must have the appropriate security clearance and have executed an **SF-312, Non-disclosure Agreement**. Contact SEC at **secinformationsecurity@usaid.gov** to obtain this form.

c. The USAID workforce must introduce, process, and store collateral classified information only in a USAID/W restricted space designated by SEC. All Top Secret (TS) and Sensitive Compartmented Information (SCI) material must be managed in a designated Sensitive Compartmented Information Facilities (SCIF). TS and SCI material may not be processed, stored, or discussed in restricted spaces.

d. Overseas Missions are not authorized to process or store classified information outside of the designated Controlled Access Area (CAA) of the U.S. Embassy. Exceptions for overseas Missions must be approved, in writing, by D/SEC (see **ADS 562, Physical Security Programs (Overseas)**, for additional information).

e. The USAID workforce must not make available to, nor leave classified information in the custody of foreign nationals. Members of the workforce must not permit foreign nationals to attend meetings where classified information is discussed or directly provide any classified information, verbally or non-verbally, to foreign nationals.

f. The USAID workforce must process classified information only on those computer systems expressly approved for processing classified information. The USAID workforce must adhere to the approved level of classification permitted for processing on the identified system. Secret and Confidential information should only be processed on approved classified information systems. TS and SCI should only be processed in designated SCIFs.

568.3.2.1 Designated Restricted and Unrestricted Spaces

Effective Date: 05/19/2017

All office areas within USAID/W headquarters and offsite facilities are designated as either "restricted" or "unrestricted". A change in designation for any office or office suite must be requested in writing by the B/IO Assistant Administrator or Office Director and sent to the SEC/CTIS Division Chief. Subsequent approval or disapproval by SEC/CTIS is based upon an inspection and evaluation of the space to determine and ensure full compliance with established standards. SEC/CTIS/IIS maintains a listing of all restricted and unrestricted office spaces. A B/IO may not change its own office from restricted to unrestricted, or vice versa. The change of space designation can only be performed by SEC. Non-SEC members of the workforce are not permitted to remove restricted or unrestricted signs that are placed at the entrances/exits to office areas.

A designated restricted space is defined as an area where storage, processing, discussions, and handling of classified material may occur. Designated restricted spaces are authorized for GSA-approved containers (safes), and classified equipment such as ThinClient terminals and STE/ViPer equipment. Upon request, SEC may grant unescorted access to designated restricted space to an authorized individual who has a valid national security clearance at the Secret level or higher. The security clearance must be properly certified and forwarded to SEC in writing by the individual's parent agency or organization. Other members of the workforce requesting access to designated restricted space must be escorted at all times by a cleared, authorized individual that has been granted "unescorted access" to the designated restricted space. Members of the workforce who are escorting others must remain with the individual(s) they are escorting at all times. Members of the workforce are not permitted to leave the individual(s) they are escorting at any point unless they turn over escort responsibilities to another authorized individual. If turning over escort responsibilities, the original escort must contact the USAID security guards and provide them with the name of the new escort. Escorted individual(s) are not permitted to be within restricted spaces without their escort at any time. Escorted individual(s) are not permitted to sit and work in restricted spaces. Failure to follow these procedures may result in a security incident for the designated escort (see **ADS 565.3.4, Visitors and Guests to USAID/W**).

A designated unrestricted space is defined as an area where the storage, processing, discussion, and handling of classified material are not authorized. Classified meetings or conversations are not authorized in designated unrestricted spaces. All USAID overseas Missions are designated as unrestricted and prohibited from storage and processing of classified information. While overseas, all classified information must be stored, processed, and discussed in the Controlled Access Area (CAA) inside the U.S. Embassy, as designated by the Regional Security Officer (RSO) (see **ADS 562.3.1**).

568.3.2.2 Sensitive Compartmented Information (SCI)

Effective Date: 05/19/2017

SEC will maintain oversight of all USAID SCIFs. Badge access to these SCIFs must be requested through SEC. Members of the workforce who have been granted SCI access will be permitted to enter and work in USAID SCIFs. These individuals will be subject to a security violation if they provide SCI to any individual who has not been cleared to that level.

Visitor access to SCIFs by foreign nationals may only be permitted if approved in writing by D/SEC. Visitor access to SCIFs by individuals without SCI will require the SCIFs to be sanitized of all SCI-related material. Members of the workforce within the SCIF will be informed that the visitor does not have SCI, and the visitor must be escorted and be within the escort's direct personal control at all times while within that space. All visitors to the SCIF must sign in and out of the Visitor Control Log. A visitor to the SCIF is considered any individual who does not have badge access into the SCIF.

Portable electronic devices (to include but not limited to cellular telephones, tablets, fitness trackers, smart watches) are not permitted within the SCIFs. The introduction of these devices in a SCIF will result in a security incident for the individual(s) involved.

SCI is regulated through Intelligence Community Directives (ICDs). ICD 704 "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information" and ICD 705 "National Intelligence" apply to all SCI that is accessed, discussed, stored, and disseminated throughout USAID.

568.3.3 Storage and Safeguarding of Classified Materials

Effective Date: 05/19/2017

Members of the workforce must ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons. USAID may impose criminal, civil, and administrative sanctions on a member of the workforce who fails to protect classified information from unauthorized disclosure (see **EO 13526 Section 5.5**).

568.3.3.1 Storage of Classified Materials

Effective Date: 05/19/2017

a. All Top Secret and SCI documents must only be handled, discussed, processed and stored in a SCIF. D/SEC must approve any exceptions in writing.

b. Members of the workforce must store Secret and Confidential material in a designated restricted space in a GSA-approved container (safe) with a GSA-approved, built-in, three-position, dial-type combination lock.

c. Classified materials may not be read, discussed, or stored in unrestricted spaces at any time.

d. Overseas Missions are not authorized to store classified materials in Mission facilities. Missions must store classified materials overseas in a GSA-approved container in the U.S. Embassy's designated Controlled Access Area (see **ADS 562, Physical Security Programs (Overseas)**).

e. Members of the workforce are responsible for reporting to the USO any malfunctioning or defective GSA-approved container in writing. The USO must immediately report defects to SEC in writing. If the safe is not immediately repaired, properly cleared individuals within that B/IO must move the classified materials to a secure location (another GSA-approved container). If a safe malfunction occurs after hours, the member of the workforce must contact the USAID Uniformed Security Officer at the Agency's 14th Street Visitor Control Desk to arrange for the proper temporary storage of classified materials. Malfunctioning or defective safes may never be left unsecured without contacting SEC and obtaining their guidance.

568.3.3.2 Security Container Combinations

Effective Date: 05/19/2017

a. SEC provides all combination change services.

b. SEC will make combination changes when:

- Security container is initially put into use;
- Security container is moved from active to inactive;
- A member of the workforce knowing the combination departs the Agency or is permanently transferred to duties which no longer require access;
- On a yearly basis as part of the Bureau/Independent Office's annual inspection;
- Upon knowledge or suspicion that the combination has been compromised; and
- If a security incident occurs involving that security container.

For any of the above occurrences, the B/IO AMS/USO must contact SEC to change the combination.

c. SEC will change computer room and communication area vault doors every six months.

d. SEC will record combinations on an **SF-700, Security Container Information** form. SEC will classify records of combinations at the highest level of classified material to be stored in the security container.

e. SEC will post the names of the custodians of the safe on the inside of the control drawer (drawer where the combination device is located) of a safe or on the inside of a vault door using an **SF-700, Security Container Information** form.

f. At a minimum, members of the workforce must store combinations and related information in repositories authorized for the storage of material at the highest combined classification level to which combinations permit access. These individuals must commit combinations to memory and must not post, write, or record combinations in an unauthorized manner.

g. Members of the workforce are not permitted to provide the combination to another individual. Only AMS/USOs and safe custodians are permitted to provide the combination to additional members of the workforce within their office. All individuals who are provided with the combination must fill out and sign the

Combination Control Roster. The Combination Control Roster must be maintained within the appropriate safe at all times. This will be an item that is inspected during the B/IO's annual inspection.

568.3.3.3 Procedures for Removing or Moving a Security Container (Safe)

Effective Date: 05/19/2017

There are many instances through which a GSA-approved container (safe) must be removed from or moved within an office space, such as when a program office moves to another space and requires their safe in the new location or when a safe is no longer needed within a B/IO. For all instances whereby a safe needs to be removed or moved, SEC/CTIS/IIS must be notified in advance and be involved in the entire process. B/IOs are not permitted to request that M/MS/HMD remove or move a safe without prior approval from SEC. Requesting the removal or movement of a safe without prior coordination and approval from SEC could result in a security incident for those involved with the request.

The combination to all new safes must be set by SEC prior to the B/IO being permitted to store classified information within that safe. Prior to a safe being removed from a B/IO, SEC must clear it to ensure there are no classified materials remaining in the safe and SEC must change the combination to factory settings.

To request the removal or movement of a safe, contact the SEC/CTIS/IIS team at **secinformationsecurity@usaid.gov**.

568.3.3.4 Security Container (Safe) Procurement

Effective Date: 05/19/2017

The General Services Administration (GSA) enacted procedures for procuring secure storage equipment, such as security containers, information processing system (IPS) containers, and vault doors. **32 CFR 2001.42 (a) Storage**, prescribes that "… whenever new secure storage equipment is procured, it must be in conformance with the standards and specifications established by the Administrator of GSA, and shall, to the maximum extent possible, be of the type available through the Federal Supply System." "GSA Approved" security containers and vault doors must now be procured through GSA Global Supply, utilizing the appropriate National Stock Number. For additional information for ordering security equipment, see: **http://www.gsa.gov/portal/content/170591**.

"GSA Approved" IPS containers must be purchased using Special Item Number 489-190 under the GSA Multiple Award Schedule program. All security storage equipment used for securing classified information must have the GSA approval label.

To request assistance with the procurement of a safe or to request a combination for a newly procured safe, contact the SEC/CTIS/IIS team at **secinformationsecurity@usaid.gov**.

568.3.3.5 Procedures for Safeguarding Classified Materials

Effective Date: 05/19/2017

Members of the workforce using classified materials are responsible for their custody and must take every precaution to prevent deliberate or casual access to it by unauthorized persons.

All classified materials must be within the individual's direct personal control at all times when not secured within a GSA-approved container (safe). Members of the workforce must not leave classified material in unoccupied rooms or inadequately protected in an occupied office, or in an office occupied by individuals without security clearances and the need to know (see **568.6**, for information on "need to know"). Open storage is not permitted at any time within restricted spaces.

SEC must pre-approve the installation and/or use of cameras, video teleconferencing equipment, web cameras, or other devices which transmit or record audio or video in USAID spaces. Members of the workforce and visitors are restricted from using such devices in USAID restricted spaces unless pre-approved by SEC in writing (see **ADS 565.3.6, Use of Cameras, Photographic or Video Teleconferencing Equipment**).

568.3.3.6 Closing Hours Security Check

Effective Date: 05/19/2017

a. The AMS/USO must issue written procedures for their respective B/IO or Mission outlining the conduct of end-of-day security checks exclusive to those conducted randomly by USAID's uniformed security guards. The assigned Duty Officer must perform these checks at the close of each business day. The purpose of these checks is to protect classified information and the safety and security of the workforce. The AMS/USO must forward a copy of these written procedures to SEC and also produce them during the B/IO's annual security inspection (see **568.3.4.10**).

Such "end-of-day" procedures must ascertain that:

- All classified equipment and material, to include that processed on any automated information system, has been properly stored in an approved GSA container and that those containers are locked;
- Windows and doors, where appropriate, are locked;
- The area is otherwise secure, alarmed (where applicable), and not susceptible to overt penetration; and

- General safety and security checks are complete.

b. Supervisory officials must designate members of the workforce (Duty Officers) to conduct a closing-hours security inspection of offices within a specifically defined area of responsibility. Such designees must use the SF-701, Activity Security Checklist, to record the results of the closing hours security check. Note: Users can obtain this form on the **Office of Security's Web site on the USAID intranet**. USOs must post the SF-701 near the main entry/exit door, and the USO must retain the SF- 701 for a period of one year to permit SEC inspection. The SF-702, Security Container Check Sheet, must be used to record the initials, time, and date in which the Duty Officer checked the GSA-approved container (safe). USOs must switch out the SF-702 at the end of each month. SF-702s may only contain one month's worth of activity. SF-702s may not contain several months' worth of activity on the same sheet. Each SF-702 must have the top portion properly filled out prior to it being placed on the safe and used by staff. USOs are responsible for filing and maintaining all SF-702s within their B/IO for one full year and providing these forms during their B/IO's annual inspection.

c. Members of the workforce designated to conduct the closing security check must report infractions of the regulations to the USO.

d. Members of the workforce designated to conduct closing hours security checks will, at a minimum:

- Ensure that all repositories containing classified material are secure;
- Ensure that an SF-702, Security Container Check Sheet, is properly annotated. Users can obtain this form on the **Office of Security's Web site on the USAID intranet**.;
- Ensure that removable classified media (e.g. data disk, CD/DVD) has been removed and is properly secured;
- Check the tops of all desks, including "in" and "out" boxes, copiers, faxes, and printers to ensure that all classified material has been secured;
- Make a visual check of the remainder of the office; and
- Ensure that an SF-701, Activity Security Checklist, is properly annotated. Users can obtain this form on the **Office of Security's Web site on the USAID intranet**; and
- Ensure the SCIF is locked and alarmed, where applicable.

e. Members of the workforce conducting closing hours checks carry a direct and important security responsibility. Although custodians of classified material are

responsible for its safekeeping, the individual performing the end-of-day check, under certain circumstances, may be jointly held responsible for certain incidents.

f. USOs must request exceptions to the foregoing requirements, based upon physical or workforce considerations, in writing to SEC. When warranted, SEC will grant approvals on a case-by-case basis.

568.3.3.7 Envelopes and Cover sheets

Effective Date: 05/19/2017

a. Except as noted in this section, members of the workforce responsible for mailing or hand- carrying classified material at the Confidential and Secret levels to addresses in the continental U.S., must ensure the material is double-wrapped in opaque envelopes or containers as follows:

- Cover classified documents with a cover sheet and enclose in two opaque envelopes.
- It is not a requirement to enclose materials transmitted overseas via the Department of State's Diplomatic Pouch service in a second or outer envelope because the pouch is considered the second or outer cover. The inner envelope is required and the outer envelope is encouraged in these instances.
- Address the inner envelope to the appropriate official by name, title, and post/organization. Mark conspicuously on both sides with the appropriate classification and include a return address. The outer envelope must never include the classification level.
- Members of the workforce must address the required outer envelope for U.S. Mail in the same manner, but without a security classification or any other indication that the contents are classified. The envelope must contain a return address but not contain a person's name. At no time will Top Secret (TS) or Sensitive Compartmented Information (SCI) information be introduced into the U.S. mail system. For assistance in transporting TS or SCI information, contact SEC. The **Office of Security Web site** contains an example of the proper marking for these envelopes.
- TS or SCI may not be removed from a SCIF unless:

  1. Authorized by the Special Security Officer (SSO) and/or Special Security Representatives (SSR);
  2. Absolutely necessary in the course of official business;
  3. It contains the proper coversheet;

4. It is double wrapped;

5. The individual removing it has a valid courier card for the level of information they will be carrying; and/or

6. The information will be transported directly to another SCIF.

b. When outside of an approved security container, classified documents must be covered with an approved color cover sheet corresponding to the highest level of classified information within the document. Under no circumstances may cover sheets be photocopied. Additional cover sheets can be ordered through GSA. The following cover sheets must be used, as appropriate:

- **SF-703, Top Secret cover sheet**;
- **SF-704, Secret cover sheet**; and
- **SF-705, Confidential cover sheet**.

568.3.3.8 Meetings and Conferences

Effective Date: 05/19/2017

Classified discussions/meetings are only permitted within designated restricted spaces in USAID/W. Members of the workforce overseas must hold classified meetings within the confines of Department of State or authorized U.S. Government controlled facilities and/or controlled access areas (CAAs) designated by the Regional Security Officer (RSO).

Meetings with Members of the USAID Workforce

In conducting meetings or conferences where classified information or material may be involved and only members of the USAID workforce will be attending, the B/IO hosting or conducting the conference must take every precaution possible to:

- Hold classified conferences only inside of a designated restricted space on official premises in the interests of national security;
- Verify attendees' security clearance levels prior to the commencement of the meeting;
- Ensure attendees are aware of the classification level of the information discussed so they can appropriately mark and safeguard any notes;
- Implement proper physical security measures to provide protection for such information or material equal to the measures required during normal operations;

- Confirm that participants are entitled to access such information; and
- Maintain a sign-in sheet/log reflecting those who attended.

Meetings with Individuals from Outside of USAID

The USAID/W B/IO hosting or conducting a classified meeting or conference must follow the above guidelines in addition to providing advance notice to their servicing USO and providing SEC with advance notice whenever it removes classified material from its normal place of storage and transmits or carries it to the conference site; or when visitors from another agency/entity are planning on attending the meeting.

Attendees of meetings at the Secret level and below are required to have their Security Office send their security clearance information to the SEC Clearance Verification Team at **SECClearanceVerif@usaid.gov**. Their attendance must be approved by SEC.

All of the above guidelines pertain to discussions/meetings within USAID/W space involving classified materials up to the Secret level. Discussions/meetings that involve Top Secret and above, including TS, SCI, and Special Access Programs (SAPs), must be held in the designated SCIFs. Attendees of meetings that will take place in the SCIFs must provide SEC/CTIS/IIS with advance notice of the discussion/meeting and also have the parent agency or organization's Security Office provide SEC/CTIS/IIS with the individual's clearance information or pertinent information for IIS to verify the clearance through the use of various clearance databases. Individuals from outside of USAID must not be permitted access to classified information/discussions/meetings at USAID without being vetted.

568.3.3.9 Transporting or Transmitting Classified Materials Within USAID Office Spaces

Effective Date: 05/19/2017

This section refers to carrying classified materials within USAID office areas without exiting the Agency turnstiles or guard posts. Once a member of the workforce exits the Agency turnstiles or guard posts, they are considered to be outside of USAID office spaces.

These individuals must ensure classified information is properly wrapped and protected before transporting it throughout the Agency, i.e. leaving restricted spaces with the classified materials. Proper wrapping for transportation within USAID office areas includes a classified cover sheet and an outer envelope or lock bag. Employees are not permitted to carry classified materials outside of any restricted space unless the materials contain the proper cover sheet and are sealed in an envelope or lock bag. Classified information may not be carried unprotected through USAID hallways.

These individuals are not permitted to bring classified materials into unrestricted spaces. Classified materials must be transported from restricted space to restricted space and properly stored in a safe when not within one's direct personal control.

Failure to properly transport classified materials within USAID office areas may result in a security incident. Following these procedures will assist with protecting classified materials from unauthorized disclosure.

568.3.3.10 Hand-Carrying Classified Information

Effective Date: 05/19/2017

Hand-carrying classified material outside of USAID/Washington facilities is highly discouraged. The preferred method for transporting/transmitting classified information is through authorized classified computer terminals.

The procedures established in this ADS chapter are to ensure proper storage, handling, transfer, and overall control of classified material leaving the Agency by way of authorized courier. In those rare instances where classified material must be hand carried, the following procedures must be followed to ensure all reasonable measures are taken to prevent the compromise of classified information through negligence, improper or indifferent security procedures.

Members of the workforce must not remove classified material from official premises except when necessary in the conduct of official meetings, conferences, or consultations and must return the material to an authorized U.S. Government owned/controlled facility and security container immediately upon the conclusion of the meeting, conference, or consultation. Individuals authorized to hand-carry classified materials must have in their possession an approved courier card. To obtain a courier card, individuals must submit a signed and completed **AID 568-1 form** to **couriercard@usaid.gov**. This card can only be issued by SEC based upon an operational requirement that is approved by the requestor's supervisor. Prior to granting courier authorization, the requestor must meet the courier training requirement. SEC will issue these cards for a period not to exceed one year and it will be based upon the requirements submitted with the request. The designated courier must also receive a courier briefing and sign an acknowledgement of responsibilities when they pick up their card in person from SEC. More information can be obtained through the **Office of Security's Information and Industrial Security Branch's Courier Card Web site**).

Members of the workforce are authorized to hand-carry classified materials up to the level listed on their valid courier card (Confidential, Secret, and Top Secret) within the Washington, DC metro area. However, due to the inherent risk of hand-carrying classified material, requirements to courier TS or SCI must be coordinated with SEC by the requestor in advance by contacting **secinformationsecurity@usaid.gov**. There are additional questions that must be answered by employees who have a valid need to hand-carry SCI.

Hand-carrying classified material is only permitted when:

- The classified material is required at the destination;
- The classified material is not available at the destination; and
- The classified material cannot be transmitted by other authorized means (listed below) due to time or other constraints.

The other approved transportation methods of classified information are:

- U.S. registered mail within the United States and the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession; and
- U.S. Postal Service Express Mail, which can only be used when it is the most effective means to accomplish a mission within security, time, cost, and accountability constraints. To ensure direct delivery to the addressee, the "Waiver of Signature" block on the United States Mail label may not be executed under any circumstances. All classified express mail shipments must be processed through mail distribution centers or delivered directly to a U.S. Postal Service facility or representative. The use of external (side street) express mail collection boxes is prohibited. Mail containing classified information, i.e., official mail, must not be sent to posts through military or diplomatic postal facilities.

Individuals hand-carrying classified documents must also adhere to the following:

- Their security clearance must be current/active;
- Their security clearance must be at least at the level of the classified information they are carrying;
- The classified material must be in the physical possession of the custodian at all times, unless proper storage at a U.S. Government facility or activity or appropriately cleared contractor facility (i.e., Continental U.S. only) is available;
- A direct route must be taken to the location in which the classified information is needed. No stops (e.g., bank, clothing store, restaurant) should be made while in the possession of the classified materials;
- The classified material must be properly wrapped and secured (i.e., double wrapped or secured in an authorized courier pouch with the proper return address with no classification level markings on the outside envelope or bag);
- Classified material must not be taken home or to a hotel for storage;
- Hand-carrying classified material on trips that involve overnight stopovers is not permitted without advance arrangements for proper overnight storage at an approved government facility or activity;

- Classified material may not be read, studied, displayed, or used in any manner on a public conveyance or in a public place;

- Classified material must not to be stored in any detachable storage compartment such as an automobile luggage rack, aircraft travel pod, or drop tank;

- Whenever possible, classified material must be returned to the parent organization by one of the approved methods of transmission;

- Trips outside the continental United States must be coordinated with SEC in advance;

- TS or SCI information may only be transmitted by either: TS cleared messenger, Authorized Courier, Department of State Courier Service, Department of Defense Courier Service, Department of State nonprofessional courier, or electronic means in approved encrypted form such as secure fax, secure telephone, or an accredited U.S. Government TS or TS/SCI approved classified system; and

- Under no circumstances may classified material be physically transmitted across international boundaries except by Department of State diplomatic courier or authorized diplomatic courier service. Nonprofessional diplomatic couriers are given such material for international transporting only in emergencies, when the professional service will not cover the area into which the pouch must be carried or the post to which the pouch is addressed within the time that official business must be conducted. In such isolated cases, the nonprofessional diplomatic courier must be in possession of a diplomatic passport and a courier letter, and the material must be enclosed in sealed diplomatic pouches until delivered to its official destination. More information on diplomatic pouches can be found through **Department of State's Web site** or within the **Mail Management Unit at the U.S. Department of State**.

568.3.3.11 Outside of USAID Office Areas

Effective Date: 05/19/2017

a. Under no circumstances will classified material be transmitted physically across international boundaries or to an overseas Mission except by the Department of State diplomatic courier or a specially authorized diplomatic courier service.

b. TS and SCI information must be transmitted by:

- Authorized TS-cleared messenger;

- Authorized courier (Department of State Courier Service, Department of Defense Courier Service (DCS), or Department of State nonprofessional courier); or

- Electronic means in approved encrypted form (such as approved secure fax, secure telephone, or an accredited U.S. Government TS or TS/SCI classified information system).

c. Secret and Confidential information may be transmitted via:

- One of the means approved for TS;
- Electronic means in approved encrypted form (such as approved secure fax, secure telephone, or classified computer system);
- U.S. Registered Mail within and between the 50 states and the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession;
- U.S. Postal Service Express Mail within and between the 50 states and the District of Columbia only when it is the most effective means to accomplish a mission within security, time, cost, and accountability constraints. To ensure direct delivery to the addressee, the "Waiver of Signature and Indemnity" block on the United States Mail label may not be executed under any circumstances; all classified express mail shipments must be processed through mail distribution centers or delivered to a U.S. Postal Service facility or representative. The use of external (side street) express mail collection boxes is prohibited; or
- U.S. Registered Mail facilities of U.S. military installations. Mail containing classified information, i.e. official mail, must not be sent to posts through military or diplomatic postal facilities (see **14 FAM 750** and **14 FAM 760** for this prohibition) (also see **12 FAM 530**).

568.3.3.12 Reproduction of Classified Material

Effective Date: 05/19/2017

Reproduction of TS information must be performed on authorized equipment within the SCIFs. The reproduction of Secret and Confidential information must only be performed on photocopy equipment specifically designated for the reproduction of classified material. SEC is responsible for posting the initial necessary signage to designated photocopy machines authorized for the reproduction of classified materials. The USO is responsible for ensuring all photocopy machines within their office are properly labeled at all times.

568.3.3.13 Destruction Procedures

Effective Date: 05/19/2017

Cleared U.S. citizens must destroy classified material, including working papers, handwritten notes, and magnetic media only through authorized means.

Domestically, approved destruction methods include cross-cut shredding and the use of the Department of State's burn bag program. SEC maintains a list of NSA-approved shredders. Bureaus/Independent Offices purchasing shredders are responsible for ensuring that the equipment is approved. The USO is responsible for marking all equipment approved for the destruction of classified materials.

Classified materials may be destroyed in burn bags, which are transported to the Department of State by the Bureau for Management, Office of Management Services, Headquarters Management Division (M/MS/HMD). Burn bags containing classified materials must be stored in a GSA-approved container and must not be left unattended. Staples and binder clips must be removed from documents prior to the documents being placed in the burn bags. Burn bags containing trash will not be accepted.

When using a burn bag, members of the workforce must separate paper from non-paper and remove all metal clips and staples. The bags must be closed with a staple and cannot be heavier than ten pounds. The bags must also be clearly labeled with the individual's name, telephone number, room number, and the highest classification level of the information within the bag. All burn bags must be labeled as soon as information is placed within them.

TS and SCI materials must be destroyed using an approved shredder located in a SCIF. TS and SCI documents or removable media may not be placed in a burn bag for pick up and disposal by M/MS/HMD. These items must be destroyed within a SCIF or coordinated with SEC for proper disposal.

Before destroying any government record, you must ensure that the required retention period has been served. You can find this information in the mandatory disposition instructions referenced in **ADS 502, The USAID Records Management Program**. Questions regarding records dispositioning should be directed to the Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD) at **recordsinquiry@usaid.gov**.

568.3.4 Security Education and Awareness

Effective Date: 05/19/2017

Establishing and maintaining an education and training program ensures that new and existing members of the workforce remain aware of their responsibilities as it concerns access to classified information.

568.3.4.1 General Requirements

Effective Date: 05/19/2017

The information security education program must include all members of the workforce who are authorized or expected to be authorized to access classified information.

The program is designed to:

- Advise the workforce of the adverse effects to national security that could result from unauthorized disclosure and of their personal and legal responsibility to protect classified information within their knowledge, possession, or control;

- Indoctrinate the workforce in the principles, criteria, and procedures of proper classification management to include classification, marking, control and accountability, storage, transmission, and destruction of classified information and material;

- Familiarize the workforce with the procedures for challenging classification decisions believed to be improper;

- Advise the workforce of the strict prohibition against discussing classified information over an unsecure telephone or through any other manner that permits interception by unauthorized persons;

- Inform the workforce of the penalties for violating or disregarding the provisions of this regulation as well as **EO 13526** and **32 CFR Parts 2001 and 2003**; and

- Instruct the workforce that individuals having knowledge, possession, or control of classified information must determine, before disseminating such information, that the prospective recipient:

    1. Has been cleared for access by competent authority;

    2. Needs the information in order to perform his or her official duties; and

    3. Can properly protect (or store) the information.

Training will be tracked by SEC/CTIS/IIS through the use of Human Capital and Talent Management's (HCTM) USAID University Learning Management System (LMS) as well as the Security Investigations Database (SID). The IIS Branch will monitor training and ensure compliance with mandatory training requirements.

568.3.4.2 Initial Security Training

Effective Date: 05/19/2017

All new or re-employed members of the workforce must attend and complete the Initial Security Briefing and sign an SF-312, Non-disclosure Agreement, prior to being afforded access to national security (classified) information. Contact SEC at **secinformationsecurity@usaid.gov** to obtain a copy of this form. It is the responsibility of the AMS to ensure that all newly assigned or newly employed members of the workforce are briefed on security matters specific to their particular assignment. Overseas, it is the responsibility of the EXO to provide training and obtain a signed SF-312, Non-disclosure Agreement. SF-312s that are signed overseas must be sent to SEC/CTIS/IIS for retention. SEC tracks and monitors all training through USAID

University.

568.3.4.3 Annual Security Refresher Training

Effective Date: 05/19/2017

Refresher training is required on an annual basis for all members of the workforce who have continued access to classified information or USAID restricted spaces. Annually, these individuals must register and complete the established SEC mandated refresher training requirements via USAID University.

The AMS, and EXO (if overseas), is required to reconcile training requirements with SEC.

Employees who do not attend this mandatory training could be subject to the following penalties:

Non-compliance	Penalty
Nonattendance of B/IO's training sessions by established/communicated due date	Letter of Concern from SEC Supervisors will be notified.
Nonattendance within 30 days of receipt of first Letter of Concern	Letter of Warning coordinated with HCTM/ELR Supervisors will be notified.

Non-compliance	Penalty
Nonattendance within 30 days of receipt of Letter of Warning	Letter of Reprimand coordinated with HCTM/ELR to Removal of physical access (USAID badge disabled and loss of access to USAID facilities) and logical access (loss of access to USAID). computer systems).

For members of the workforce who are not employed directly by USAID, comparable penalties will be coordinated with the Contracting Officer. SEC will coordinate with HCTM/ELR to determine the appropriate disciplinary action for subsequent non-compliance as per the Table of Penalties (see **ADS 487, Disciplinary and Adverse Actions Based upon Employee Misconduct – Civil Service**, **ADS 485, Disciplinary Action – Foreign Service**, and **3 FAM 4300, Disciplinary Action**).

All persons granted SCI access will be advised annually of their continuing security responsibilities. SEC/CTIS/IIS will provide annual SCI refresher training to all members of the workforce with valid SCI access. Training provided will keep individuals informed of appropriate changes in security regulations, policies, and reinforce the training provided during their initial indoctrination. When a member of the workforce receives their SCI revalidation through the SCI Requests Team within SEC's Personnel Security Division, the individual will be contacted by the IIS Branch to complete their SCI refresher training. This training must be completed within 15 business days of notice by IIS, unless otherwise authorized in writing by SEC. IIS will maintain records of training and enter them into SID, when applicable.

SCI is regulated through Intelligence Community Directives (ICDs). ICD 704 "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information" and ICD 705 "National Intelligence" apply to all SCI that is accessed, discussed, stored, and disseminated throughout USAID (see **ICD 704** and **ICD 705**).

568.3.4.4 Original Classification Authority (OCA) Training

Effective Date: 05/19/2017

SEC will provide training for all OCAs. All original classification authorities must receive training in proper classification (including the avoidance of over-classification) and declassification as provided in **EO 13526** and its implementing directives at least once each calendar year. This training will include instructions on the proper safeguarding of classified information and on the sanctions in section 5.5 of **EO 13526** that may be brought against an individual who fails to classify information properly or protect

classified information from unauthorized disclosure. Original classification authorities who do not receive such mandatory training at least once within a calendar year will have their classification authority suspended by the agency head or D/SEC (as per section 5.4(d) of **EO 13526**) until such training has taken place. A written waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual must receive such training as soon as practicable.

568.3.4.5 Derivative Classification Authority Training

Effective Date: 05/19/2017

SEC provides derivative classification training in the proper application of the derivative classification principles of **EO 13526** and **32 CFR Parts 2001 and 2003** prior to derivatively classifying information. All members of the workforce who apply derivative classification markings are required to attend training every year. Derivative classifiers who do not receive such training at least once every year must have their authority to apply derivative classification markings suspended until they have received such training.

568.3.4.6 Unit Security Officer (USO) Training

Effective Date: 05/19/2017

The B/IO head must delegate the USO in writing to SEC. In Missions overseas, this responsibility generally is delegated to the Executive Officer (EXO). SEC provides monthly and quarterly training for USOs. All B/IOs will be required to have a designated USO attend each monthly training session as well as one of the quarterly sessions every year. It will be acceptable for either the Primary or the Alternate USO to attend the monthly meetings and report back to the other designee who was unable to attend. However, all new USOs will be required to attend the first quarterly session that is offered after they are appointed. All delegated USOs will be required to attend one quarterly training session each year to maintain their designation as a USO.

568.3.4.7 Special Access

Effective Date: 05/19/2017

SEC/CTIS/IIS provides initial indoctrination briefings for members of the workforce who are authorized access to Sensitive Compartmented Information (SCI) or Special Access Programs (SAPs). Annually, all U.S. Direct-Hires and PSCs, who were granted SCI through USAID, must complete an SCI refresher training (see **568.3.4.3**).

568.3.4.8 Termination Briefings (Debriefings)

Effective Date: 05/19/2017

SEC must provide a security debriefing to all employees granted access to National Security information. The mandatory debriefing ensures that separating employees are aware of their responsibilities for returning all classified material and of a continuing responsibility to safeguard the classified information with which they were previously entrusted. Individuals must also turn in their USAID issued identification card(s) at this time. Overseas, the EXO is responsible for debriefing employees and forwarding a separation statement and Non-disclosure Agreement (i.e. SF-312, Form 4414), to the SEC/CTIS/IIS Branch. Contact SEC at **secinformationsecurity@usaid.gov** to obtain these forms (see **ADS 451** for more information on the debriefing process).

568.3.4.9 Separation Overseas

Effective Date: 05/19/2017

Overseas, the USAID Mission Unit Security Officer must ensure that members of the workforce cleared for access to classified information are given a local/Mission security briefing upon arrival, and prior to departure, and a debriefing to ensure that they understand security requirements.

- All members of the workforce cleared for access to classified information must sign the SF-312, Classified Information Non-disclosure Agreement, when initially briefed. Signed SF-312s must be sent to the Office of Security's Information and Industrial Security Branch at **secinformationsecurity@usaid.gov**.

- When departing USAID, overseas employees must either sign the debriefing section of the SF-312 overseas and ensure it is sent to **secinformationsecurity@usaid.gov** or visit SEC and sign the debriefing section of the SF-312 (see **ADS 451**, **ADS 303**, and **ADS 306** for more about the separation process).

568.3.4.10 Security Inspections

Effective Date: 05/19/2017

EO 13526 Part 5, Implementation and Review requires agencies to conduct regular self-inspections to evaluate procedures to safeguard Classified National Security Information. As the designated Senior Agency Official for information security, D/SEC is responsible for implementation and monitoring of the Agency Security Inspection Program. This program may use a range of mechanisms, including a formal annual inspection, routine and non-routine after-hours checks, and unannounced inspections. To conduct these inspections, SEC and the Bureau for Management, Chief Information Security Officer (M/CISO) staff have the authority to open offices, desk drawers, security containers, etc., to gain access to classified or other sensitive information or materials in hard copy and electronic form when necessary to support a security inspection or investigation.

Although USAID will protect the privacy of specific personally identifiable information as required by law, individuals have no reasonable expectation of privacy in:

- The USAID workplace,
- Work-related items in the workplace,
- U.S. Government-owned property, or
- USAID security containers.

SEC and M/CISO staff and affiliated members of the workforce designated by SEC have the authority to conduct searches in these locations without consent or a warrant, for work- related purposes, to ensure compliance with national and local agency security policies, or as part of an investigation for work-related misconduct.

Cleared U.S. citizen security members of the workforce designated by SEC are responsible for conducting security inspections to ensure that classified information is properly protected. Items covered during the Security Inspection Program include, but are not limited to, the following areas:

- Classification activities;
- Representative sample of classification actions (original and derivative);
- Access, handling, and dissemination of classified materials;
- Security containers and their contents;
- Classified equipment (for example, classified printers, Communication Security (COMSEC) equipment and secured telephones);
- Equipment used for classified reproduction and destruction;
- Doors, alarms, and locking mechanisms;
- Access granted to visitors and members of the workforce;
- End-of-day check procedures;
- Destruction procedures;
- Security training; and
- Adequate SEC and M/CIO/CISO audit trails.

Relevant findings from the Security Inspection Program (self-inspections) are reported by SEC/CTIS directly to the B/IO head, AMS, and USO. The AMS/USO is responsible for taking immediate corrective action to resolve all findings within an established timeframe

from receipt of the written report. The established timeframe is determined by SEC and communicated in the 30/60/90 day plan that will be provided during the out-briefing. SEC will conduct a follow-up inspection after 30/60/90 days, as previously stated, to ensure that recommended corrective actions have been adequately addressed. Self-inspection activities and findings are also reported annually, around November of each year, to the Information Security Oversight Office (ISOO) through the Self-Inspection Report.

For additional guidance or details on the self-inspection program, see **ISOO Directive 1; section 2001.60**.

568.3.5 Security Incident Program

Effective Date: 05/19/2017

The purpose of the Security Incident Program is to enhance the protection of classified information by identifying, evaluating, and assigning responsibility for breaches of security.

Members of the USAID workforce who commit security infractions or violations, or a supervisor who fails to enforce effective organizational security procedures, may be subject to administrative, disciplinary, or security clearance actions, as appropriate, by HCTM, SEC, and/or M/CISO staff. When the infraction is committed by a contractor, any actions must be coordinated through the Contracting Officer. Recommendations for disciplinary and/or security clearance actions will be handled on a case-by-case basis and will be influenced by the severity of the incident and the security history of the offender.

To facilitate the management of the Security Incident Program, SEC and M/CISO staff will maintain files on all members of the workforce who have incurred security infractions or security violations. Security infractions or violations represent performance inconsistent with the expectations and criteria for awarding a performance bonus or promotion.

Following the affirmative adjudication of either a security infraction or a security violation, a 36-month moving window will be established from the date of the most recent infraction/violation.

The window will look backwards and allow HCTM, SEC, or contracting officials to consider previous infractions/violations within the 36-month window in administrative or disciplinary rulings. A security infraction/violation may be considered a second time if it occurs within 36 months of another incident.

568.3.5.1 Reporting Security Incidents

Effective Date: 05/19/2017

a. Members of the workforce and USAID Guard Force staff must immediately report all security incidents to SEC/CTIS/IIS. In overseas Missions, security incidents

must be reported to the Executive Officer and SEC/CTIS/IIS. SEC will collaborate with M/CISO staff regarding any computer related incidents. Members of the workforce must inform the appropriate AMS or USO, orally or in writing, of any improper security practice that comes to the workforce's attention in order to facilitate remedial action.

b. Upon notification of a security incident, SEC/CTIS/IIS will perform a preliminary inquiry into the incident. If it is determined that there was an infraction or violation committed, SEC/CTIS/IIS will complete a warning letter and Form OF-118, Record of Incident. Contact SEC at **secinformationsecurity@usaid.gov** to obtain a copy of this form. The SEC representative will provide the warning letter and OF-118 to the subject of the incident who will then execute and sign the Form OF-118, section 2, within three workdays. Section 2 of the OF-118 allows the subject to provide any mitigating factors which he or she believes are pertinent to the adjudication process. If the subject of the incident fails or refuses to sign the form within three workdays, the SEC representative will document this fact in section 3 of the OF-118.

When the individual listed in section 1a of the OF-118 signs section 2, the SEC representative or the individual listed in section 1a will give the form to the subject's immediate supervisor for signature. For overseas Missions, the RSO will complete the investigation and the OF-118, and provide it to SEC. If the RSO does not characterize the incident as either an infraction or violation, SEC will do so and upload it into the individual's SID file, if applicable (see **568.3.5.3**).

c. Upon completion of the OF-118, Record of Incident, SEC/CTIS/IIS must generate an official warning letter to the individual. SEC must forward a copy of this letter to the AMS. SEC must also retain a copy of the OF-118 and the official warning letter and these documents will be uploaded and retained in the individual's clearance file within SID.

d. For any incident involving a visitor, contractor, or individual from another government agency, SEC will notify the parent company or organization's security office in writing. When applicable, SEC must also notify the USAID Contracting Officer's Representative (COR) and the Contracting Officer (CO).

568.3.5.2 Examples of Security Incidents

Effective Date: 05/19/2017

Listed in this section are examples of security incidents that affect the protection of classified information. The examples are intended to illustrate the wide range of possible security incidents. These examples are not intended to list all possible categories/scenarios.

Examples of security incidents are as follows:

- Failing to properly escort visitors or allowing improper access to USAID restricted

spaces;

- Taking classified material out of the building without proper double-wrap protection and an authorized courier card;
- Carrying classified information around USAID/W spaces (outside of the restricted space in which it resided) without a proper cover sheet and envelope or lock bag;
- Failing to secure GSA-approved containers with classified materials;
- Failing to keep an open/unsecured GSA-approved container within one's direct line of sight at all times;
- Unsecured GSA-approved container left unattended;
- Storing classified material in desk drawers or other improper containers;
- Failing to properly secure classified removable media;
- Reading, discussing, storing, handling, or sharing classified materials in any public or unrestricted space;
- Transmitting classified material on an unclassified facsimile machine;
- Reproducing classified material on unauthorized equipment;
- Transmitting or transporting classified material in an unauthorized manner;
- Placing classified information on an unclassified or unauthorized system;
- Losing control of classified material by leaving it in non-secure areas such as hotel rooms, taxis, or restaurants;
- Discussing classified information on unsecure telephones or in unrestricted spaces;
- Providing unauthorized individual(s) access to classified information;
- Storing classified information in an unrestricted space; and
- Processing or storing classified information at an overseas Mission or any designated unrestricted space, unless that Mission or B/IO has received special written authorization from SEC.

568.3.5.3 Categorization of Security Incidents

Effective Date: 05/19/2017

Security incidents are investigated and adjudicated as a Practice Dangerous to Security (PDS), security infraction, or violation.

A PDS is an act that does not meet the standards of a security infraction or violation, but has the potential to jeopardize the security of sensitive information or operations if allowed to continue.

A security infraction is the failure to properly safeguard classified materials that does not result in the actual or probable compromise of the material (for example, improperly stored classified material within a controlled access area or designated restricted space).

A security violation is the failure to properly safeguard information classified at the Confidential or Secret level that results in the actual or probable compromise of the material, or any security incident involving mishandling of TS, Special Access Program, or SCI, regardless of the location or probability of compromise.

All security incidents, to include PDS, will be reported immediately to SEC.

SEC must notify the originating agency and other departments or agencies that may have equity in the lost or compromised classified national security information. SEC must notify the Office of the Director of National Intelligence (ODNI), through the National Counterintelligence Executive (NCIX), within 48 hours of any security incident involving the actual or probable loss or compromise of SCI.

A damage assessment may be conducted by, and at the discretion of, the originating agency when there is an actual or suspected unauthorized disclosure or compromise of classified national security information. The damage assessment will be used to evaluate actual or potential damage to national security resulting from the unauthorized disclosure or compromise of classified national security information which may adversely affect national security.

568.3.5.4 Disciplinary Actions and Security Clearance Review Related to PDS and Security Infractions

Effective Date: 05/19/2017

a. Following an affirmative adjudication by SEC that a PDS or security infraction has occurred, SEC/CTIS will review the incident, along with a summary of mitigating or aggravating factors and other security incidents within the moving 36-month window. In addition to its own review, SEC may also refer the matter to HCTM for disciplinary action.

b. For the first PDS or infraction, the SEC/CTIS/IIS Chief will send a letter of warning to the offender. The offender is required to send a written reply acknowledging that he or she understands the policies and ramifications of future security incidents. The offender may be required to attend security training, as directed by SEC.

c. For a second PDS or infraction within 36 months, the SEC/CTIS/IIS Chief will send the offender a warning letter that includes a statement concerning the actions SEC will take in the event of future security incidents. This letter will require a signed response from the offender acknowledging the ramifications of future security incidents. The offender will be required to attend security training, as directed by SEC.

d. A third or subsequent PDS or infraction within the 36-month window will result in the Deputy Director of SEC referring the matter to HCTM for possible disciplinary action and a concurrent review within SEC to determine the offender's continued eligibility to hold a security clearance.

568.3.5.5 Disciplinary Actions and Security Clearance Review Related to Security Violations

Effective Date: 05/19/2017

a. Following an affirmative adjudication by SEC/CTIS/IIS that a security violation has occurred, SEC/CTIS will review the incident, along with a summary of mitigating or aggravating factors and other security incidents within the moving 36-month window. In addition to its own review, SEC may also refer the matter to HCTM for disciplinary action.

b. As part of its review, SEC/CTIS/IIS may issue a letter of warning, and refer the security incident to the Personnel Security Division for review and adjudication of the incident for continued eligibility for security clearance.

c. HCTM may issue a letter of admonishment or reprimand, suspend the violator without pay, or terminate employment.

d. If the violator is a contractor, or a PSC, SEC/CTIS/IIS will notify the cognizant Contracting or Agreement Officer to take appropriate action in accordance with the terms of the contract or grant/cooperative agreement.

Incidents involving intentional or grossly negligent mishandling of classified information may subject the offender to criminal penalties.

568.3.5.6 Appeals of Security Incidents

Effective Date: 05/19/2017

Individuals wishing to appeal the validity or categorization of a security incident may submit their appeal in writing to SEC/CTIS/IIS.

- The appeal must be dated within 30 days of the written warning letter from SEC/CTIS/IIS of the decision to assign responsibility for the incident.

- Upon receipt of the appeal, SEC/CTIS/IIS will forward it to the SEC/CTIS Division Chief for a decision. A member of the workforce's statement on Form OF-118, Record of Incident, does not initiate the appeal process. Contact SEC at **secinformationsecurity@usaid.gov** to obtain this form. SEC will respond to appeals within 30 days of their receipt by SEC.

- M/CIO/CISO will be involved in the appeals of incidents involving information systems.

568.3.6 Processing Classified National Security Information on USAID Automated Systems

Effective Date: 05/19/2017

In USAID/Washington, members of the workforce must process Classified National Security Information on dedicated classified computer systems, microprocessors approved to process such information, or on a Department of State approved network (see the AMS Officer for current locations of approved classified computer systems).

The processing, storing, printing, or transmitting of classified information on any unauthorized network or unauthorized computer system is strictly prohibited and may constitute a security incident. Additional policies and procedures are found in **ADS 552, Classified Information Systems Security**. All known or suspected instances of processing classified national security information on an unclassified information system must be immediately reported to SEC and M/CIO/CISO.

568.3.7 Counterintelligence

Effective Date: 05/19/2017

The Office of Security's Counterintelligence (CI) Branch is responsible for detecting, deterring, and neutralizing the threat from Foreign Intelligence Services (FIS) and terrorists. SEC/CI enhances the long-term security and safety of members of the workforce and programs worldwide by identifying and mitigating counterintelligence threats to these individuals and operations through defensive measures. Additional policies and procedures are found in **ADS 569, Counterintelligence Program.**

568.4 MANDATORY REFERENCES

568.4.1 External Mandatory References

Effective Date: 05/19/2017

a. **5 USC 552b(1)**

b. **12 FAM 262, Security Awareness and Contact Reporting, and 263,**

Counterintelligence Awareness Program (These contain the policy and procedures for USAID implementation of PDD/NSC-12, Security Awareness and Reporting of Foreign Contacts, of August 5, 1993.)

c. **12 FAM 264, Personal Travel to Critical Human Intelligence Threat Countries, November 30, 1994**

d. **12 FAM 500, Information Security** (This contains the policy and procedures for USAID implementation of EO 13526 concerning classified information.)

e. **12 FAM 557.1, Record Keeping and Administrative Action Framework**

f. **December 29, 2009, "Presidential Memoranda – Implementation of Executive Order, Classified National Security Information"**

g. **EO 12968, "Access to Classified Information," of August 4, 1995, as amended by EO 13467 "Reforming Processes to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information**

h. **EO 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information"**

i. **EO 13526, "Classified National Security Information" of December 29, 2009**

j. **Federal Information Processing Standards, Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS 201), March 2006**

k. **Homeland Security Presidential Directive-12 (HSPD-12), August 27, 2004**

l. **Information Security Oversight Office (ISOO) Directive, 32 C.F.R. Part 2001, June 25, 2010**

m. **Intelligence Community Directives (ICD) 704 "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information" and ICD 705 "National Intelligence"**

n. **Marking Classified National Security Information, ISOO Publication**

o. **National Industrial Security Program Operating Manual (NISPOM)**

p. **PDD/NSC-12, "Security Awareness and Reporting of Foreign Contacts," of August 5, 1993**

q. **Section 587(b) of the Fiscal Year 1999 Omnibus Appropriations Bill (Pub. L. 105-277)**

568.4.2 Internal Mandatory References

Effective Date: 05/19/2017

a. **ADS 309, Personal Services Contracts with Individuals**

b. **ADS 544, Technical Architecture Design, Development, and Management**

c. **ADS 550, End-User Applications**

d. **ADS 552, Classified Information Systems Security**

e. **ADS 562, Physical Security Programs (Overseas)**

f. **ADS 566, Personnel Security Investigations and Clearances**

g. **ADS 567, Classified Contracts and Awards Under USAID's National Industrial Security Program**

h. **ADS 569, Counterintelligence**

i. **USAID Classification Guide**

568.4.3 Mandatory Forms

Effective Date: 05/19/2017

a. AID 568-1, Courier Card Request Form [Contact the Office of Security (SEC) at: **secinformationsecurity@usaid.gov** or go to the IIS Branch Web site: **https://pages.usaid.gov/SEC/courier-card** to obtain a copy of this form.]

b. OF-118, Record of Incident [Contact the Office of Security (SEC) at: **secinformationsecurity@usaid.gov** to obtain a copy of this form.]

c. SF-311, Agency Security Classification Management Program Data [Contact the Office of Security (SEC) at: **secinformationsecurity@usaid.gov** to obtain a copy of this form.]

d. SF-312, Classified Information Non-disclosure Agreement [Contact the Office of Security (SEC) at: **secinformationsecurity@usaid.gov** to obtain a copy of this form.]

e. SF-700, Security Container Information [Contact the Office of Security (SEC) at: **secinformationsecurity@usaid.gov** to obtain a copy of this form.]

f. SF-701, Activity Security Checklist [Contact the Office of Security (SEC) at:

secinformationsecurity@usaid.gov to obtain a copy of this form.]

g. SF-702, Security Container Check Sheet [Contact the Office of Security (SEC) at: **secinformationsecurity@usaid.gov** to obtain a copy of this form.]

h. SF-703, Top Secret Cover Sheet [Contact the Office of Security (SEC) at: **secinformationsecurity@usaid.gov** to obtain a copy of this form.]

i. SF-704, Secret Cover Sheet [Contact the Office of Security (SEC) at: **secinformationsecurity@usaid.gov** to obtain a copy of this form.]

j. SF-705, Confidential Cover Sheet [Contact the Office of Security (SEC) at: **secinformationsecurity@usaid.gov** to obtain a copy of this form.]

568.5 ADDITIONAL HELP

Effective Date: 05/19/2017

a. Information Security Questions – **secinformationsecurity@usaid.gov**

b. Information Systems Security Questions (computer systems) – **ISSO@usaid.gov**

568.6 DEFINITIONS

Effective Date: 05/19/2017

See the **ADS Glossary** for all ADS terms and definitions.

access
The ability and opportunity to obtain knowledge of classified information. An individual is considered to have access by being in a place where national security information is kept, processed, handled, or discussed, if the security control measures that are in force do not prevent that person from gaining knowledge of such information. (**Chapters 562**, **566**, **567**, **568**)

classification guide
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. (**Chapter 562** and **568**)

Classified National Security Information (Classified Information)
Any media or data (regardless of its form), file, paper, record, disk, removable media or computer screen containing information associated with the national defense or foreign relations of the United States and bearing the markings: Confidential, Secret, or Top Secret. (**Chapters 545**, **552**, **568**)

Information that has been determined pursuant to **EO 13526** or any predecessor order to require protection against unauthorized disclosure and is marked (Confidential, Secret, or Top Secret) to indicate its classified status when in documentary form. It is also referred to as classified information.

a. Confidential: The unauthorized disclosure of information which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

b. Secret: Information of which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

c. Top Secret: Information of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. (Chapters **545**, **552**, **562**, **566**, **567**)

Collateral Classified National Security Information
Classified information which has no supplemental or additional handling restrictions. (**Chapter 568**)

Communications Security (COMSEC)
Measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications. COMSEC includes crypto-security, transmission security, emissions security, and physical security of COMSEC material and information. (**Chapter 562** and **568**)

counterintelligence
Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, persons or international terrorist activities, excluding personnel, physical, document, and communications security programs. (**Chapters 562**, **568**, **569**)

derivative classification
The act of reproducing, extracting, or summarizing classified information, or applying classification markings derived from source material or as directed by a classification guide. (**EO 13526**) (**Chapter 568**)

escort
Accompany (someone or something) somewhere, especially for protection or security, or as a mark of rank. (**Chapter 568**)

Executive Officer (EXO)
Serves as a Unit Security Officer overseas, responsible to both SEC and the post RSO. Collaborates with the Chief Information Officer (CIO) as the Information Systems Security Officer (ISSO) in ensuring USAID compliance with USAID and Post security directives. (**Chapter 568**)

marking
The physical act of indicating on national security information the proper classification levels, the classification authority, the agency and office of origin, declassification and downgrading instructions, and special markings which limit the use of the classified information. (**Chapter 562** and **568**)

need to know
A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform official duties. The determination is not made solely by virtue of an individual's office, position, or security clearance level. (**Chapters 562**, **566**, **567**, **568**)

open storage
A room or area constructed for the purpose of safeguarding national security information that, because of its size or nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers. Open storage rooms permit classified information to be outside of a GSA-approved container when not within one's direct personal control. (**Chapter 568**)

original classification
An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. (**Chapter 562** and **568**)

Original Classification Authority (OCA)
An individual authorized in writing, either by the President, or by Agency heads or other officials designated by the President, to classify information in the first instance. (**Chapters 562**, **566**, **568**)

over-classification
When a piece of information is classified at a level higher than it should be to adequately protect national security. (**Chapter 568**)

Practice Dangerous to Security (PDS)
Practices which have the potential to jeopardize the security of sensitive information or operations if allowed to continue. (**Chapter 568**)

restricted space
An area where storage, processing, discussions, and handling of classified documents is authorized. (**Chapters 565**, **567**, **568**)

removable media
Items such as thumb drives, CDs, and removable hard drives that connect to a computer system to transfer information and can later be removed from that computer system. (**Chapter 568**)

security classification guide
A document prepared for the sole or principal purpose of providing instructions about

the derivative classification of information about a particular program, project, or subject. (**Chapters 562**, **567**, **568**)

security incident
An event that results in the failure to safeguard classified materials in accordance with **EO 13526**, "Classified National Security Information," 12 FAM 500, and **ADS 566**. The consequence of a security incident is either a PDS, a security infraction, or a security violation. (**Chapter 568**)

security infraction
A failure to properly safeguard classified material that does not result in the actual or probable compromise of the material, for example, improperly stored classified material within a controlled access area. (**Chapter 568**)

security violation
A failure to properly safeguard confidential or secret classified material that results in the actual or probable compromise of the material, or any security incident involving the mishandling of Top Secret, Special Access Program, and Special Compartmented Information, regardless of location or probability of compromise. (**Chapter 568**)

Sensitive Compartmented Information Facility (SCIF)
A SCIF is an accredited area, room, group of rooms, buildings, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed. SCIFs will be afforded access control to preclude entry by unauthorized person(s). (**Chapter 568**)

Special Access Program (SAP)
A sensitive program, approved in writing by a head of Agency with original top secret classification authority, that imposes need to know and access controls beyond those normally provided for access to confidential, secret, or top secret information. (**Chapter 568**)

unrestricted space
An area where storage, processing, discussion, and handling of classified documents is not authorized. (**Chapter 565** and **568**)

USAID/W
Refers to all Washington, DC office locations, including but not limited to, the Ronald Reagan Building, SA-44, and Potomac Yards. (**Chapter 568**)

568_051917