



ADS Chapter 568

National Security Information Program

Full Revision Date: 01/25/2012
Responsible Office: SEC/OD
File Name: 568_012512

**Functional Series 500 - Management Services
Chapter 568 - National Security Information Program**

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

Table of Contents

568.1 OVERVIEW 4

568.2 PRIMARY RESPONSIBILITIES 4

568.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES..... 5

568.3.1 Classification of National Security Information 5

568.3.1.1 Original Classification Authority 5

568.3.1.2 Classification Challenges..... 6

568.3.1.3 Classification Guide 7

568.3.1.4 Annual Summary Preparation..... 7

568.3.1.5 Identification and Marking..... 8

568.3.1.6 SEC Review..... 8

568.3.1.7 FOIA Review..... 9

568.3.2 Access, Control, and Dissemination..... 9

568.3.3 Storage and Safeguarding of Classified Materials..... 10

568.3.3.1 Storage of Classified Materials 10

568.3.3.2 Security Container Combinations 11

568.3.3.3 Procedures for Safeguarding Classified Materials 11

568.3.3.4 Closing Hours Security Check 12

568.3.3.5 Envelopes and Covers..... 13

568.3.3.6 Meetings and Conferences..... 14

568.3.3.7 Transporting or Transmission of Classified Materials 15

568.3.3.8 Hand-Carrying Classified Information 16

568.3.3.9 Reproduction of Classified Material 18

568.3.3.10 Destruction Procedures 19

568.3.4 Security Education and Awareness 19

568.3.4.1 General Requirements..... 19

568.3.4.2 Initial Security Training..... 20

568.3.4.3 Annual Refresher Training 20

568.3.4.4 Original Classification Authority (OCA) Training 21

568.3.4.5 Derivative Classification Authority Training..... 21

568.3.4.6 Unit Security Officer (USO) Training..... 22

568.3.4.7 Special Access 22

568.3.4.8 Termination Briefings..... 22

<u>568.3.4.9</u>	<u>Security Inspections</u>	<u>22</u>
<u>568.3.5</u>	<u>Security Incident Program</u>	<u>24</u>
<u>568.3.5.1</u>	<u>Reporting Security Incidents</u>	<u>24</u>
<u>568.3.5.2</u>	<u>Examples of Security Incidents</u>	<u>25</u>
<u>568.3.5.3</u>	<u>Categorization of Security Incidents</u>	<u>26</u>
<u>568.3.5.4</u>	<u>Disciplinary Actions and Security Clearance Review Related to PDS and Security Infractions</u>	<u>26</u>
<u>568.3.5.5</u>	<u>Disciplinary Actions and Security Clearance Review Related to Security Violations</u>	<u>27</u>
<u>568.3.5.6</u>	<u>Appeals of Security Incidents</u>	<u>27</u>
<u>568.3.5.7</u>	<u>Contractor Personnel Overseas</u>	<u>28</u>
<u>568.3.6</u>	<u>Processing National Security (Classified) USAID Automated Systems</u>	<u>28</u>
<u>568.3.7</u>	<u>Counterintelligence</u>	<u>28</u>
<u>568.4</u>	<u>MANDATORY REFERENCES</u>	<u>29</u>
<u>568.4.1</u>	<u>External Mandatory References</u>	<u>29</u>
<u>568.4.2</u>	<u>Internal Mandatory References</u>	<u>30</u>
<u>568.4.3</u>	<u>Mandatory Forms</u>	<u>30</u>
<u>568.5</u>	<u>ADDITIONAL HELP</u>	<u>31</u>
<u>568.6</u>	<u>DEFINITIONS</u>	<u>31</u>

Chapter 568 - National Security Information Program

568.1 OVERVIEW

Effective Date: 01/23/2012

This ADS chapter provides the policy directives and required procedures for USAID's implementation of [Executive Order \(E.O.\) 13526, Classified National Security Information](#); [E.O. 12968, Access to Classified Information](#); [E.O. 12829, National Industrial Security Program](#); [National Industrial Security Program Operating Manual \(NISPOM\)](#); and [12 FAM 500, Information Security](#).

Throughout this chapter, the term USAID employees refers to all employees that work for USAID, including but not limited to direct-hires and Personal Services Contractors (PSCs).

568.2 PRIMARY RESPONSIBILITIES

Effective Date: 01/23/2012

- a. **The USAID Director of Security (D/SEC)** is the USAID senior Agency official under Executive Orders 13526 and 12968. The responsibilities of the senior Agency official are stipulated in each of the E.O.s (see [E.O. 13526](#), [E.O. 12968](#), and [E.O. 12829](#)).
- b. **Chief, Counter-Terrorism Information and Industrial Security (CTIS) Division** is responsible for overseeing and implementing program policies and responsibilities related to the Information and Industrial Security (IIS) program.
- c. **The Executive Secretary (ES) of the Agency** is responsible for establishing and maintaining a system of accounting for Top Secret material (see [E.O. 13526](#)). Additionally, the ES has Unit Security Officer responsibilities for USAID Sensitive Compartmented Information Facilities.
- d. **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).
- e. **The Unit Security Officer (USO)** is responsible for ensuring that all operations within his or her respective Mission and Bureau/Independent Offices (B/IOs) are carried out in accordance with the security regulations in this chapter.
- f. **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.

g. The Original Classification Authority (OCA) is responsible for annual review of the USAID Classification Guide and the proper conduct and documentation of classification decisions within their respective B/IOs.

h. Office of Human Resources, Employee Labor Relations (OHR/ELR) is responsible for coordinating with SEC for formal disciplinary actions for noncompliance with policies.

568.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

This section contains the mandatory policies and required procedures for ADS Chapter 568.

568.3.1 Classification of National Security Information

Effective Date: 01/23/2012

[12 FAM 500](#) contains the policy and procedures for USAID and all foreign affairs agencies concerning the implementation of E.O. 13526. The policies and required procedures in this chapter supplement 12 FAM 500 for USAID and must be considered in conjunction with 12 FAM 500 and Executive Order 13526 (see [12 FAM 500](#) and [E.O. 13526](#)).

The head of each B/IO and overseas USAID Mission must appoint a Unit Security Officer. Individuals with original classification authority; security managers or security specialists; and personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings, will be evaluated for this activity during the annual performance period. This requirement also applies to USAID staff including but not limited to Executive Officers (EXOs), AMs, USOs, and personnel within A/AID, 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.

568.3.1.1 Original Classification Authority

Effective Date: 01/23/2012

As prescribed in [E.O. 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 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 (OCA) 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 [E.O. 13526](#) is strictly limited. USAID officials do not have the authority to classify at the Top Secret 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).

The head of each B/IO and OCA must conduct an annual review of the USAID Classification Guide (a copy of the USAID Classification Guide may be obtained by contacting the SEC Counterterrorism and Information Security Division (SEC/CTIS/IIS)) and either attest to its adequacy or draft and submit recommended changes in writing to SEC. 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.

In order to ensure the appropriateness of classifications, the respective AMS officials for A/AID, DA/AID, and IG must maintain a log of all classified decisions made annually, which includes the classification level, document type, reviewer's name, and date of classification decision. The log must be submitted to SEC for review at the end of each fiscal year but no later than October 15.

[**Note:** All employees with a security clearance possess derivative classification authority. [E.O. 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." [E.O. 13526](#), section 2.1 and the Information Security Oversight Office's booklet entitled [Marking Classified National Security Information](#) (October 2007) outline the procedures for exercising derivative classification and marking of documents.]

568.3.1.2 Classification Challenges

Effective Date: 01/23/2012

If holders or recipients of classified information have substantial reason to believe that the information is improperly classified or, in fact, is unclassified, they must communicate that belief to the classifier of the information. The classification authority block will identify the classifier of the information on the classified document as indicated in **568.3.1.5**.

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

Employees may submit 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. Employees accessing the classified computer systems must have a security clearance, attend a mandatory training on how to properly use the system, and sign a user agreement certifying that he or she will secure classified removable media.

OCAs receiving challenges pursuant to this section must act upon them within 30 calendar days of receipt. 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. If resolution cannot be obtained within the Agency, further appeal may be made to the Information Security Oversight Office (ISOO) Classification Appeals Panel.

Employees may direct allegations, or complaints regarding over-classification or incorrect classification within the agency to D/SEC through written documentation or electronically using the secure classified computer systems.

568.3.1.3 Classification Guide Effective Date: 01/23/2012

USAID's Classification Guide (USCG) can be used by all USAID employees to derivatively classify information. As per [E.O. 13526](#), an individual is determined to have derivative classification authority if they have the appropriate security clearance and have attended derivative classification training every two years.

568.3.1.4 Annual Summary Preparation Effective Date: 01/12/2009

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.

All Bureaus/Independent Offices (B/IOs) must maintain a centralized log file of all original (if applicable) and derivative classification activity which includes all information required on the [SF-311, Agency Security Classification Management Program Data](#).

Using this centralized file, the AMS Officer is responsible for providing annual classification activity statistics to SEC. The AMS must prepare and submit to SEC a form AID 500-8, Annual Summary of Classification Activity **[Note: This document is only available on the USAID intranet]**. All B/IOs must submit the form to SEC no later than October 15 of each year for inclusion in the Agency's annual report to the ISOO.

568.3.1.5 Identification and Marking

Effective Date: 01/23/2012

All personnel must identify and mark all classified material as provided in Section 1.6 of **E.O. 13526**. Paper documents markings must not deviate from the format prescribed in **E.O. 13526** and the Information Security Oversight Office's booklet entitled [Marking Classified National Security Information](#) (October 2007). This booklet addresses the following topics related to markings:

- Classification standards,
- Classification prohibitions and limitations,
- Classification challenges,
- Classification guides,
- Fundamental classification guidance review,
- One of the three classification levels,
- Portion markings,
- The identity of the classification authority and office of origin, and
- The date or event for declassification.

568.3.1.6 SEC Review

Effective Date: 01/23/2012

At SEC's request, B/IOs must make all classified documents 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), all employees that derivatively or originally classify documents are required to maintain an unclassified record reflecting the number of documents classified, if they were originally or derivatively classified, and the level of classification.

568.3.1.7 FOIA Review

Effective Date: 01/12/2009

Recipients of FOIA requests involving classified information must direct the requests in writing to SEC/CTIS/IIS for review and concurrence.

SEC has the authority to exercise the national security exemption as set forth in the [Freedom of Information Act, 5 U.S.C. 552b \(1\)](#) when responding to FOIA requests. SEC must verify that the information involved clearly meets the standards for continued classification irrespective of the markings, to include declassification instructions, contained in the document.

568.3.2 Access, Control, and Dissemination

Effective Date: 01/23/2012

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.

The Executive Secretary (ES) must designate the Top Secret Control Officer (TSCO) and alternate TSCO in writing to D/SEC. The ES TSCO will be responsible for the 6th floor Sensitive Compartmented Information Facility (SCIF). SEC will be responsible for the 2nd floor SCIF. The TSCO and alternate TSCO must undergo annual training presented by SEC. The TSCO is responsible for the positive control over the movement, use, and disposition of all hard copy documents/materials at the Top Secret level and above, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs). This positive control requirement also includes those documents/materials printed from automated information systems. The TSCO is responsible for duties outlined in [12 FAM 530, "Storing and Safeguarding Classified Materials."](#) SEC will provide oversight.

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 **Form SF-312**, Nondisclosure Agreement [**Note: Contact SEC to obtain this form.**]

c. USAID employees must introduce, process, and store classified information only in a designated USAID/W restricted area designated by SEC.

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. USAID employees must not make available to, nor leave classified information in the custody of foreign nationals. USAID employees 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. USAID employees must process classified information only on those computer systems expressly approved for processing classified information. USAID employees 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. Top Secret and above, such as Sensitive Compartmented Information (SCI), should only be processed in designated Sensitive Compartmented Information Facilities (SCIFs).

568.3.3 Storage and Safeguarding of Classified Materials

Effective Date: 01/12/2009

Employees 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 an employee who fails to protect classified information from unauthorized disclosure. **[Note: See Executive Order 13526 Section 5.5.]**

568.3.3.1 Storage of Classified Materials

Effective Date: 01/23/2012

a. As outlined in sub-paragraph **568.3.2** above, there must be a designated Top Secret Control Officer (TSCO) for the Agency. The TSCO, in accordance with [Section 2001.43 of ISOO Directive 1](#), must store Top Secret documents in a designated restricted area in a General Services Administration (GSA)-approved security container with a GSA-approved, built-in, three-position, dial-type combination lock. The security container must be located either in a USAID-approved alarmed area or in a building controlled by cleared U.S. citizen personnel on a 24-hour basis. SEC **must** approve any exceptions.

b. USAID employees must store Secret and Confidential material in a designated restricted area in a GSA-approved container with a GSA-approved, built-in, three-position, dial-type combination lock.

c. 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 (CAA) (see [ADS 562](#)).

d. Employees are responsible for reporting to the USO any malfunctioning or defective GSA-approved container. The USO must immediately report defects to SEC. If the safe is not immediately repaired, employees must move classified materials to a

secure location (that is, to another GSA-approved container). If a safe malfunction occurs after hours, the employee 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.

568.3.3.2 Security Container Combinations

Effective Date: 01/23/2012

- a. SEC provides all combination change services.
- b. SEC will make combination changes when
 - The security container is initially put into use;
 - An employee knowing the combination terminates employment or is permanently transferred to duties which no longer require the employee's access; and
 - Upon knowledge or suspicion that the combination has been compromised.

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

- c. SEC will change all security container combinations at least once every 12 months (except for computer room and communication area vault doors, which must be changed every six months), or when containers are moved from active to inactive service.
- d. SEC will record combinations on **Form SF-700**, Security Container Information. SEC will classify records of combinations at the highest level of classified material to be stored in the security container.
- e. At a minimum, employees 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. Employees must commit combinations to memory and must not post, write, or record combinations in an unauthorized manner.
- f. 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 **Form SF-700**.

568.3.3.3 Procedures for Safeguarding Classified Materials

Effective Date: 01/12/2009

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

Employees 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 section **568.6**, Definitions, for information on “need to know.”)

SEC must pre-approve the use of cameras, video teleconferencing equipment, or photographic equipment in designated restricted areas. Employees/visitors are restricted from using the camera feature of their personally owned telephones in restricted USAID space. (See **ADS 565.3.6 Use of Cameras, Photographic or Video Teleconferencing Equipment.**)

568.3.3.4 Closing Hours Security Check

Effective Date: 01/23/2012

a. The AMS/USO must issue written procedures for their respective Bureau/Independent Office (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 employees. The AMS/USO must forward a copy of these written procedures to SEC.

Such “end-of-day” procedures must ascertain that

- (1) 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;
- (2) Windows and doors, where appropriate, are locked;
- (3) The area is otherwise secure, alarmed (where applicable), and not susceptible to overt penetration; and
- (4) General safety and security checks are complete.

b. In order to fulfill this fundamental mandatory requirement in all areas, supervisory officials must designate employees (Duty Officers) to conduct a closing-hours security inspection of offices within a specifically defined area of responsibility. Such designees must use **Form 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.]** Unit Security Officers (USOs) must post the Form 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.

c. An employee designated to conduct the closing security check must report infractions of the regulations to the USO.

- d. Employees designated to conduct closing hour security checks will, at a minimum
- (1) Ensure that all repositories containing classified material are secure;
 - (2) Ensure that **Form SF-702**, Security Container Check Sheet, is properly annotated [**Note: Users can obtain this form on the Office of Security's Web site on the USAID intranet**];
 - (3) Ensure that removable classified media has been removed and is properly secured;
 - (4) Check the tops of all desks, including "in" and "out" boxes, copiers, faxes, and printers to ensure that all classified material has been secured;
 - (5) Make a visual check of the remainder of the office; and
 - (6) Ensure that Form SF-701, Activity Security Checklist, is properly annotated [**Note: Users can obtain this form on the Office of Security's Web site on the USAID intranet**].
- e. Employees conducting closing-hours checks carry a direct and important security responsibility. Although custodians of classified material are responsible for its safekeeping, the employee 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 personnel considerations, in writing to SEC. When warranted, SEC will grant approvals on a case-by-case basis.

568.3.3.5 Envelopes and Covers

Effective Date: 01/12/2009

- a. Except as noted in this section, employees 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:
- (1) Cover classified documents with a cover sheet and enclose in an opaque envelope.
 - (2) It is not necessary 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.

(3) 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.

(4) Employees 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 information be introduced into the U.S. mail system. For assistance in transporting Top Secret information, contact SEC. **[Note: The Office of Security Web site contains an example of the proper marking for these envelopes.]**

b. When outside of an approved security container, cover classified documents with an approved cover sheet, as follows:

- SF-703, Top Secret cover sheet
- SF-704, Secret cover sheet
- SF-705, Confidential cover sheet

568.3.3.6 Meetings and Conferences

Effective Date: 01/23/2012

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

a. Meetings with USAID Personnel

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

- (1) Hold classified conferences only inside a designated restricted area on official premises, in the interests of technical security;
- (2) Verify attendees' security clearance levels prior to the commencement of the meeting;
- (3) Implement proper physical security measures to provide protection for such information or material equal to the measures required during normal operations; and
- (4) Confirm that participants are entitled to access such information.

b. 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

- (1) It removes classified material from its normal place of storage and transmits or carries it to the conference site;
- (2) Visitors from another agency/entity are planning on attending the meeting;
 - a. These attendees are required to send their security clearance information to the SEC Clearance Verification Team at SECClearanceVerif@usaid.gov.
 - b. Their attendance must be approved by SEC.
- (3) The validity of participants' security clearances is not personally known by the office hosting or conducting the classified meeting.

All of the above guidelines pertain to discussions/meetings within USAID/W space involving classified materials up to the Secret level. Top Secret (TS) and above, including TS/Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs), must be held in the designated Sensitive Compartmented Information Facilities (SCIFs). Attendees of meetings that will take place in the SCIFs must also follow the guidelines outlined above.

568.3.3.7 Transporting or Transmission of Classified Materials

Effective Date: 01/12/2009

- 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. Top Secret information must be transmitted by
 - (1) Top Secret-cleared messenger;
 - (2) Authorized courier (Department of State Courier Service, Department of Defense Courier Service (DCS), or Department of State nonprofessional courier); or
 - (3) 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

- (1) One of the means approved for Top Secret;
- (2) Electronic means in approved encrypted form (such as approved secure fax, secure telephone, or classified computer system);
- (3) 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;
- (4) 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); or
- (5) U.S. Registered Mail facilities of the Army, Navy, Air Force, or other U.S. post offices outside the areas enumerated above, provided that the material does not, at any time, pass out of the U.S. citizen employee's control and does not pass through a foreign postal system.

568.3.3.8 Hand-Carrying Classified Information

Effective Date: 01/23/2012

The hand carrying of 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 herein 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.

Employees 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 a Courier Authorization Card [**Note: Contact INFOSEC@usaid.gov to obtain this card**]. This card can only be issued by SEC once the requestor has obtained supervisory approval and has articulated an official 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 receive a courier briefing and sign an acknowledgement of responsibilities.

Employees are only authorized to hand-carry classified materials at the Secret and Confidential level around the Washington, D.C. metro area when:

- The classified material is required at the destination;
- The classified material is not available at the destination;
- 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;
- 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;
- The classified material must be in the physical possession of the custodian at all times, unless proper storage at a U.S. Government 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);

- Classified material will 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 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 is 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;
- For trips outside the continental United States, follow the requirements of ADS 568 for designation as a nonprofessional courier;
- Under no circumstances may Top Secret materials be hand carried. Top Secret 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 Electrical means in approved encrypted form such as secure fax, secure telephone, or an accredited U.S. Government TS or TS/SCI approved classified system;
- 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 pouch can be found at <http://pouch.a.state.gov> or within the Customer Service Unit, Diplomatic Pouch and mail at Department of State.

568.3.3.9 Reproduction of Classified Material

Effective Date: 01/23/2012

Only the Top Secret Control Officer (TSCO) may reproduce Top Secret information. Reproduction must be performed on authorized equipment within the Sensitive

Compartmented Information Facilities (SCIFs). The reproduction of Secret and Confidential information will be performed only 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.

568.3.3.10 Destruction Procedures

Effective Date: 01/12/2009

Cleared U.S. citizen employees 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, Management Services, Facilities Management Division (M/MS/FMD). Burn bags containing classified materials must be stored in a GSA-approved container and must not be left unattended.

Only the TSCO may destroy original Top Secret Materials. The TSCO is required to record the destruction of Top Secret material and retain those records for a period of five years from the date of destruction.

568.3.4 Security Education and Awareness

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

568.3.4.1 General Requirements

Effective Date: 01/12/2009

The information security education program must include all Direct-Hire and Personal Services Contractor (PSC) personnel, and individual experts and consultants acquired through a Bureau for Management, Office of Acquisitions and Assistance (M/OAA) issued purchase order, provided the individual(s) are authorized or expected to be authorized access to classified information. The program is designed to

- Advise personnel 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 personnel 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 personnel with the procedures for challenging classification decisions believed to be improper;
- Advise personnel of the strict prohibition against discussing classified information over an unsecure telephone or through any other manner that permits interception by unauthorized persons;
- Inform personnel of the penalties for violating or disregarding the provisions of this regulation; and
- Instruct personnel 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.

568.3.4.2 Initial Security Training

Effective Date: 01/12/2009

All new or re-employed Direct-Hire personnel, PSCs, , and Purchase Order Contractors (Experts/Consultants) must attend and complete the Initial Security Briefing and sign the **Form SF-312**, Nondisclosure Agreement, prior to being afforded access to national security (classified) information [**Note: Contact SEC to obtain a copy of this form**]. It is the responsibility of the Administrative Management Specialist (AMS) to ensure that all newly assigned or newly employed personnel 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 Form SF-312, Nondisclosure Agreement.

568.3.4.3 Annual Refresher Training

Effective Date: 01/23/2012

Refresher training is required on an annual basis for all U.S. Direct Hires and Personal Services Contractors (including Experts and Consultants described above) having continued access to classified information. The AMS is required to coordinate such training for the Bureau/Independent Office and provide SEC with annual written certification that this training requirement has been met.

Overseas, the EXO is responsible for ensuring that such training is conducted or delivered to employees and must certify annually that this training requirement has been met.

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

Non-compliance Activity	Penalty
Nonattendance of B/IO's training sessions	Letter of Reprimand issued to employee. Employee's supervisor notified.
Nonattendance within 30 days of receipt of first Letter of Reprimand	Second Letter of Reprimand to Suspension issued to employee. Employee's supervisor notified.
Nonattendance within 30 days of receipt of second Letter of Reprimand	Suspension to Removal of access (USAID Badge disabled) to USAID Facilities

SEC will coordinate with OHR/ELR to determine the appropriate disciplinary action for subsequent non-compliance as per the Table of Penalties. [Note: [ADS 487](#), Disciplinary and Adverse Actions Based upon Employee Misconduct – Civil Service and [ADS 485](#), Disciplinary Action – Foreign Service, and [3 FAM 4300](#), Disciplinary Action.]

568.3.4.4 Original Classification Authority (OCA) Training

Effective Date: 01/23/2012

SEC will provide training for all OCAs. All OCAs must receive training in proper classification and declassification prior to originally classifying information and at least once each calendar year thereafter.

568.3.4.5 Derivative Classification Authority Training

Effective Date: 01/23/2012

SEC provides derivative classification training in the proper application of the derivative classification principles of [E.O. 13526](#) prior to derivatively classifying information. All employees who apply derivative classification markings are required to attend training every two years. Derivative classifiers who do not receive such training at least once every two years 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: 01/12/2009

SEC provides training for new USOs. The B/IO head must delegate the USO in writing to SEC. Each newly designated USO is required to attend such training within 90 days of their written appointment, unless told otherwise by SEC.

568.3.4.7 Special Access

Effective Date: 01/12/2009

SEC/CTIS/IIS provides initial indoctrination briefings for personnel authorized access to Sensitive Compartment Information.

568.3.4.8 Termination Briefings

Effective Date: 01/12/2009

SEC must provide a security debriefing to all U.S. Direct-Hire employees, Personal Services Contractors, and Purchase Order Contractors granted access to National Security information. The mandatory debriefing ensures that separating personnel 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. Overseas, the EXO is responsible for debriefing the employee/contractor and forwarding a separation statement and SF 312, Classified Information Nondisclosure Agreement, to SEC [**Note: Contact SEC to obtain this form**].

568.3.4.9 Security Inspections

Effective Date: 01/23/2012

[Executive Order 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 M/CIO/CISO have the authority to open offices, desk drawers, security containers, etc., to gain access to classified or other sensitive information or materials when necessary to support a security inspection or investigation.

Although USAID will protect the privacy of specific personally identifiable information as required by law, employees 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/CIO/CISO staff and affiliated personnel 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 personnel 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;
- Access, handling, and dissemination of classified materials;
- Security containers and their contents;
- Classified equipment (for example, classified computer systems, Communication Security (COMSEC) equipment and secured telephones);
- Doors, alarms, and locking mechanisms;
- Access granted to visitors and employees;
- 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 are reported by SEC/CTIS directly to the B/IO head and AMS Officer. The AMS Officer is responsible for taking immediate corrective action on all findings.

For additional guidance or details on the self-inspection program, reference [ISOO Directive 1; section 2001.60](#).

568.3.5 Security Incident Program

Effective Date: 01/23/2012

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.

Employees 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 the Office of Human Resources (OHR), the Office of Acquisition and Assistance, SEC and/or M/CIO/CISO. 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/CIO/CISO will maintain files on all personnel 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 OHR, 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: 01/23/2012

a. Employees and USAID Guard Force staff must immediately report all security incidents to SEC/CTIS/IIS. SEC will collaborate with M/CIO/CISO regarding any computer related incidents. Employees must inform the appropriate AMS or USO, orally or in writing, of any improper security practice that comes to the employee's attention in order to facilitate remedial action.

b. Upon notification of a security incident, SEC/CTIS/IIS will investigate the incident and complete a Form OF-118, Record of Incident [**Note: Contact SEC to obtain a copy of this form**]. The SEC security officer will provide the OF-118 to the person alleged to be responsible for the incident who will then execute and sign the **Form OF-118**, Item 2, within three workdays. Item 2 of the OF-118 allows the suspected violator an opportunity to provide any mitigating factors which he or she believes are pertinent to the adjudication process. If the person alleged to be responsible for the incident fails or refuses to sign the form within three workdays, the SEC security officer will document this fact on Item 3 of the OF-118.

When the individual responsible for the incident signs the form, the SEC security officer will give the form to the employee's immediate supervisor for signature and then complete Item 3, including a brief summary indicating whether in his or her view there has been a valid security incident and, if so, whether it should be considered a security infraction or violation. For overseas Missions, the RSO will complete the investigation and the OF-118, and SEC will characterize the incident as an "infraction" or "violation" (see **568.3.5.4**).

c. Upon completion of the OF-118, Record of Incident, SEC/CTIS/IIS must generate an official warning letter to the employee. 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.

d. For any incident involving a visitor, institutional contractor, or employee of another Government agency, SEC must notify the parent company or organization's security office in writing. When applicable, SEC must also notify the USAID Contracting Officer's Representative (COR).

568.3.5.2 Examples of Security Incidents

Effective Date: 01/23/2012

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:

1. Failing to properly escort visitors or allowing improper access to USAID restricted areas;
2. Taking classified material out of the building without proper double-wrap protection and an authorized courier card;
3. Failing to secure containers with classified materials;
4. Storing classified material in desk drawers or other improper containers;
5. Failing to properly secure classified computer hard drives, diskettes, or other classified media;
6. Reading, discussing, or sharing classified materials in any public or unrestricted area;
7. Transmitting classified material on an unclassified facsimile machine;
8. Transmitting or transporting classified material in an unauthorized manner;

9. Placing classified information on an unclassified or unauthorized system;
10. Losing control of classified material by leaving it in non-secure areas such as hotel rooms, taxis, or restaurants;
11. Discussing classified information on unsecure telephones;
12. Providing unauthorized individual(s) access to classified information;
13. Storing classified information in an unrestricted area; and
14. Processing or storing classified information at an overseas Mission or any designated unrestricted area, unless that Mission or B/IO has received special written authorization from SEC.

568.3.5.3 Categorization of Security Incidents

Effective Date: 01/23/2012

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

A PDS is an act which does not comprise a security infraction or violation, but has the potential to jeopardize the security of sensitive information or operations if allowed to continue. All security incidents, to include PDS, will be reported immediately to SEC.

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 area).

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 Top Secret, Special Access Program, or Sensitive Compartmented Information, regardless of the location or probability of compromise.

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

Effective Date: 01/12/2009

- a. Following an affirmative adjudication by SEC that a security incident has occurred, SEC will review the offender's record for other security incidents within the previous 36 months.
- 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 (DD) of SEC referring the matter to OHR 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: 01/12/2009

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 HR for disciplinary action.

b. As part of its review, SEC/CTIS/IIS may issue a letter of warning, suspend the security clearance, and/or recommend to the DD/SEC that the violator's security clearance be revoked.

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

d. If the violator is a contractor, recipient employee, or a Personal Services Contractor, 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: 01/23/2012

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 SEC/CTIS for a decision. An employee statement on **Form OF-118**, Record of Incident,

does not initiate the appeal process [**Note: Contact SEC to obtain this form**].

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

568.3.5.7 Contractor Personnel Overseas

Effective Date: 01/23/2012

Overseas, the USAID Mission Unit Security Officer (USO) must ensure that U.S. citizen Personal Service Contractors (USPSCs), independent contractors, and other contractor employees cleared for access to classified information are given a local/Mission security briefing upon arrival, and prior to departure, a debriefing to ensure that they understand security requirements.

- All USAID USPSC and Purchase Order-type U.S. citizen contractor personnel must sign the **Form SF-312**, Classified Information Nondisclosure Agreement, when initially briefed [**Note: Contact SEC to obtain this form**].
- When departing USAID, the employee must visit SEC and sign the debriefing section of the Form SF-312.

568.3.6 Processing National Security (Classified) USAID Automated Systems

Effective Date: 01/23/2012

In USAID/Washington (USAID/W), employees 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 violation. Additional policies and procedures are found in [ADS 552, Classified Information Systems Security](#).

568.3.7 Counterintelligence

Effective Date: 01/23/2012

The Office of Security Counterintelligence (CI) 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 USAID personnel and programs worldwide by identifying and mitigating CI threats to personnel 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: 01/23/2012

- a. [Executive Order \(E.O.\) 13526, "Classified National Security Information" of December 29, 2009](#)
- b. [Director of Central Intelligence Directive 1/20, "Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information \(SCI\)," of December 29, 1991](#)
- c. [E.O. 12829, "National Industrial Security Program," of January 6, 1993](#)
- d. [December 29, 2009, "Presidential Memoranda – Implementation of Executive Order, Classified National Security Information"](#)
- e. [E.O. 12968, "Access to Classified Information," of August 4, 1995](#)
- f. [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.)
- g. [12 FAM 264, Personal Travel to Critical Human Intelligence Threat Countries, November 30, 1994](#)
- h. [12 FAM 500, Information Security](#) (This contains the policy and procedures for USAID implementation of E.O. 12958 concerning classified information.)
- i. [12 FAM 557.1, Record Keeping and Administrative Action Framework](#)
- j. [Marking Classified National Security Information, ISOO Publication](#)
- k. [Information Security Oversight Office \(ISOO\) Directive, 32 C.F.R. Part 2001, June 25, 2010](#)
- l. [PDD/NSC-12, "Security Awareness and Reporting of Foreign Contacts," of August 5, 1993](#)
- m. [Section 587\(b\) of the Fiscal Year 1999 Omnibus Appropriations Bill \(Pub.L. 105-277\)](#)
- n. [Homeland Security Presidential Directive-12 \(HSPD-12\), August 27, 2004](#)
- o. [Federal Information Processing Standards, Personal Identity Verification \(PIV\) of Federal Employees and Contractors \(FIPS 201\), March 2006](#)

p. [5 U.S.C. 552b\(1\)](#)

q. [National Industrial Security Program Operating Manual \(NISPOM\)](#)

568.4.2 Internal Mandatory References

Effective Date: 01/23/2012

a. [ADS 544, Technical Architecture Design, Development, and Management](#)

b. [ADS 550, End-User Applications](#)

c. [ADS 551, Data Administration](#)

d. [ADS 552, Classified Information Systems Security](#)

e. [ADS 562, Physical Security Programs \(Overseas\)](#)

f. [ADS 566, US Direct-Hire and PASA/RSSA Personnel Security Program](#)

g. [ADS 567, Classified Contracts, Grants, Cooperative Agreements, and Contractor/Recipient Personnel Security](#)

h. [ADS 569, Counterintelligence](#)

568.4.3 Mandatory Forms

Effective Date: 01/23/2012

a. **AID 500-7, Courier Authorization Card [Note: Contact the Office of Security (SEC) to obtain this form.]**

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

c. [SF-311, Agency Security Classification Management Program Data](#)

d. **SF-312, Classified Information Nondisclosure Agreement [This form is only available on the USAID intranet]**

e. **SF-700, Security Container Information [Note: Contact the Office of Security (SEC) to obtain this form.]**

f. **SF-701, Activity Security Checklist [Note: Contact the Office of Security (SEC) to obtain this form.]**

g. **SF-702, Security Container Check Sheet [Note: Contact the Office of Security (SEC) to obtain this form.]**

- h. **SF-703, Top Secret Cover Sheet [Note: Contact the Office of Security (SEC) to obtain this form.]**
- i. **SF-704, Secret Cover Sheet [Note: Contact the Office of Security (SEC) to obtain this form.]**
- j. **SF-705, Confidential Cover Sheet [Note: Contact the Office of Security (SEC) to obtain this form.]**

568.5 ADDITIONAL HELP
Effective Date: 01/23/2012

Information Security Questions – INFOSEC@usaid.gov

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

568.6 DEFINITIONS
Effective Date: 01/23/2012

The terms and definitions listed below have been included in the ADS Glossary. See the ADS Glossary for all ADS terms and definitions. (See [ADS Glossary](#))

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](#), [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. (Chapters [562](#), [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](#), and [568](#))

Information that has been determined pursuant to [E.O. 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: 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.
- 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](#))

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](#))

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. ([E.O. 13526](#))

Executive Officer (EXO)

Unit Security Officer, responsible to both SEC and the post RSO, ensuring USAID compliance with USAID and Post security directives.

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. (Chapters [562](#), [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](#))

Original Classification

An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. (Chapters [562](#), [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](#))

Practice Dangerous to Security (PDS)

Practices which have the potential to jeopardize the security of sensitive information or operations if allowed to continue.

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.

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 Executive Order 12958, "Classified National Security Information," 12 FAM 500, and ADS 566. The consequence of a security incident is either 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 personnel access control to preclude entry by unauthorized personnel.

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.

USAID/W

Refers to all Washington, D.C. office locations, including but not limited to the Ronald Reagan Building, SA-44, and Potomac Yards.

568_012512