ADS Chapter 568

National Security Information Program

Revision Date: 01/12/2009
Responsible Office: SEC/OD
File Name: 568_011209

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

***This chapter has been substantively 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 Security 5
568.3.1.1 Original Classification Authority 5
568.3.1.2 Classification Challenges 6
568.3.1.3 Annual Summary Preparation 7
568.3.1.4 Identification and Marking 7
568.3.1.5 SEC Review 7
568.3.1.6 FOIA Review 8

568.3.2 Access, Control, and Dissemination 8

568.3.3 Storage and Safeguarding of Classified Materials 9
568.3.3.1 Storage of Classified Materials 9
568.3.3.2 Security Container Combinations 10
568.3.3.3 Procedures for Safeguarding Classified 10
568.3.3.4 Closing Hours Security Check 11
568.3.3.5 Envelopes and Covers 12
568.3.3.6 Meetings and Conferences 13
568.3.3.7 Transporting or Transmission of Classified Materials 13
568.3.3.8 Hand-Carrying Classified Information 14
568.3.3.9 Reproduction of Classified 15
568.3.3.10 Destruction Procedures 15

568.3.4 Security Education and Awareness 15
568.3.4.1 General Requirements 15
568.3.4.2 Initial Security Training 16
568.3.4.3 Annual Refresher Training 17
568.3.4.4 Unit Security Officer Training (USO) 17
568.3.4.5 Special Access 17
568.3.4.6 Termination Briefings 17

568.3.5 Security Incident Program 17
568.3.5.1 Reporting Security Incidents 18
568.3.5.2 Security Inspections 19

568.3.5.3 Examples of Security Incidents 20
568.3.5.4 Categorization of Security Incidents 21
568.3.5.5 Disciplinary Actions and Security Clearance Review Related to Security Infractions 21
568.3.5.6 Disciplinary Actions and Security Clearance Review Related to Security Violations 22
568.3.5.7 Appeals of Security Incidents 22
568.3.5.8 Contractor Personnel Overseas 23

568.3.6 Processing National Security (Classified) USAID Automated Systems 23

568.3.7 Counterintelligence 23

568.4 MANDATORY REFERENCES 23

568.4.1 External Mandatory References 23

568.4.2 Internal Mandatory References 24

568.4.3 Mandatory Forms 25

568.5 ADDITIONAL HELP 25

568.6 DEFINITIONS 25

Chapter 568 - National Security Information Program

568.1 OVERVIEW

Effective Date: 01/12/09

This ADS chapter provides the policy directives and required procedures for USAID's implementation of Executive Orders (E.O.) **12958 "Classified National Security Information"**, **E.O. 12968 "Access to Classified Information"** and **E.O. 12829 "National Industrial Security Program"; National Industrial Security Program Operating Manual (NISPOM)**, and **12 FAM 500 "Information Security."**

568.2 PRIMARY RESPONSIBILITIES

Effective Date: 01/12/09

a. The USAID Director of Security (D/SEC) is the USAID senior Agency official under Executive Orders 12958 and 12968. The responsibilities of the senior Agency official are stipulated in each of the E.O.s (see **E.O. 12958, E.O. 12968,** and **E.O. 12829**).

b. The Executive Secretary (ES) is responsible for establishing and maintaining a system of accounting for Top Secret material (see **E.O. 12958**). Additionally, the ES has Unit Security Officer responsibilities for USAID Sensitive Compartmented Information Facilities.

c. The Bureau for Management, Office of Administrative Services, Information and Records Division (M/AS/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).

d. 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.

e. The Administrative Management Specialist (AMS) is responsible for coordination and documentation of classification activity; end-of-day security checks; training; and corrective actions related to security incidents or findings.

f. 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).

568.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES
Effective Date: 01/12/09

568.3.1 Classification of National Security Information Security
Effective Date: 01/12/09

12 FAM 500 contains the policy and procedures for USAID and all foreign affairs agencies concerning the implementation of E.O. 12958. 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 12958 (see **12 FAM 500** and **E.O. 12958**).

The head of each B/IO and overseas USAID Mission must appoint a Unit Security Officer.

568.3.1.1 Original Classification Authority
Effective Date: 01/12/09

As prescribed in E.O. 12958, 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) shall 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 OCA shall be in writing and the authority shall not be re-delegated except as provided in **E.O. 12958**.

The number of USAID officials possessing original classification authority as outlined in E.O. 12958 is strictly limited. USAID officials do not have the authority to classify at the Top Secret level. The Administrator (A/AID) has the authority to originally classify information at the Confidential and Secret level as the Agency Head. 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 Bureau/Independent Office (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/IS) and either attest to its adequacy or draft and submit in writing to SEC recommended changes. 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. 12958** 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. 12958, 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: 01/12/09

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 classifier of the information should be identified on the classified document as indicated in **568.3.1.4**.)

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.

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.

568.3.1.3 Annual Summary Preparation
Effective Date: 01/12/09

The Bureau for Management, Office of Administrative Services, Information and Records Division (M/AS/IRD) will prepare an annual summary of all documents reviewed and declassified during the fiscal year. M/AS/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 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 ISOO.

568.3.1.4 Identification and Marking
Effective Date: 01/12/09

All personnel must identify and mark all classified material as provided in Section 1.6 of E.O. 12958. Paper documents markings must not deviate from the format prescribed in E.O. 12958 and the Information Security Oversight Office's booklet entitled **Marking Classified National Security Information** (October 2007). These markings include the following:

- 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.

568.3.1.5 SEC Review
Effective Date: 01/12/09

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.

In USAID/Washington, A/AID, DA/AID, and IG must maintain a centralized file containing a copy of all classified documents produced within their respective B/IO. The file must be stored in a General Services Administration (GSA)-approved security container with a GSA-approved, built-in, three-position, dial-type combination lock.

568.3.1.6 FOIA Review
Effective Date: 01/12/09

Recipients of FOIA requests involving classified information must direct the requests in writing to SEC/CTIS/IS 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: 01/12/09

a. ES must designate the Top Secret Control Officer (TSCO) in writing to D/SEC. The TSCO is responsible for the positive control over the movement, use, and disposition of all Top Secret documents/material, to include those housed on automated information systems. The TSCO is responsible for duties outlined in **12 FAM 535, "Storing and Safeguarding Classified Materials."**

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: This form can be obtained by contacting SEC**].

c. USAID employees and contractors must introduce, process, and store classified information only in a designated USAID/Washington (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 or contractors must not make available to, nor leave classified information in the custody of foreign nationals. USAID employees or contractors must not permit foreign nationals to attend meetings where classified information is disclosed. Foreign nationals may not receive dictation of or otherwise type classified information.

f. USAID employees or contractors 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.

568.3.3 Storage and Safeguarding of Classified Materials
Effective Date: 01/12/09

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.

568.3.3.1 Storage of Classified Materials
Effective Date: 01/12/09

a. As outlined in sub-paragraph **568.3.2** above, the ES must designate the Top Secret Control Officer (TSCO) for the Agency in writing. The TSCO, in accordance with **Section 4.4 of E.O. 12958**, 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 an 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 or contractors must store Secret and Confidential material in a designated restricted area in the same manner as authorized for Top Secret information

- in a GSA-approved container with a GSA-approved, built-in, three-position, dial-type combination lock; or

- in an area approved for the open storage of classified materials.

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 or contractors 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: 01/12/09

a. Only individuals having an appropriate security clearance will change combinations to security containers and vaults. Domestically, SEC provides combination change services.

b. Employees or 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.

c. The combinations of all security containers must be changed 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. Employees or contractors must record combinations on Form SF-700, Security Container Information [**Note: This form can be obtained by contacting SEC**]. Employees or contractors will classify records of combinations at the highest level of classified material to be stored in the security container.

e. At a minimum, employees or contractors 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 and contractors must commit combinations to memory and must not post, write, or record combinations in an unauthorized manner.

f. The names of personnel having knowledge of the combination must be posted 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
Effective Date: 01/12/09

Employees and contractors 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 and contractors 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.

568.3.3.4 Closing Hours Security Check

Effective Date: 01/12/09

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. These checks must be performed at the close of each business day. 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; and

(3) The area is otherwise secure and not susceptible to overt penetration.

b. In order to fulfill this fundamental mandatory requirement in all areas, supervisory officials must designate employees 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: This form can be obtained by contacting SEC**]. 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: This form can be obtained by contacting SEC**];

(3) Ensure that removable hard drives to classified information systems have been removed and are 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: This form can be obtained by contacting SEC**].

e. Employees conducting closing-hours checks carry a direct and important security responsibility. Although custodians of classified material are responsible for its safekeeping, the checker, under certain circumstances, may be jointly held responsible for the violation.

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

568.3.3.5 Envelopes and Covers

Effective Date: 01/12/09

a. Except as noted in this section, employees or contractors 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) Classified documents must be covered by a cover sheet or folded inward and be enclosed in an opaque envelope.

(2) Materials transmitted overseas via the Department of State’s Diplomatic Pouch service need not be enclosed 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. It must be marked conspicuously on both sides with the appropriate classification and contain 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.

b. Classified documents must be covered with an approved cover sheet, as follows:

- SF-703, Top Secret cover sheet
- SF-704, Secret cover sheet
- SF-705, Confidential cover sheet for when information is not physically stored in an approved security container.

568.3.3.6 Meetings and Conferences
Effective Date: 01/12/09

Classified meetings are permitted to be conducted only within a designated restricted area in USAID/W. Overseas, classified meetings must be held within the confines of a controlled access area (CAA) designated by the Regional Security Officer (RSO) for classified meetings.

a. In conducting meetings or conferences where classified information or material may be involved, the (B/IO) calling or conducting the conference must observe every precaution to ensure that

(1) In the interests of technical security, classified conferences are held only inside a designated restricted area on official premises;

(2) Proper physical security measures are implemented to provide protection for such information or material equal to the measures required during normal operations; and

(3) Participants are entitled to access such information.

b. The USAID/W Bureau/Independent Office hosting or conducting a classified meeting or conference must give advance notice to and coordinate with their servicing USO and provide SEC with advance notice whenever

(1) Classified material is to be removed from its normal place of storage and transmitted or carried to the conference site; or

(2) The validity of participants' security clearances is not personally known by the office hosting or conducting the classified meeting.

568.3.3.7 Transporting or Transmission of Classified Materials
Effective Date: 01/12/09

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 nonprofessional diplomatic courier service.

b. Top Secret information must be transmitted by either

(1) Top Secret-cleared messenger;

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

(3) Electronic means in approved encrypted form (such as approved secure fax, secure telephone, or Intelink).

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 ClassNet);

(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 must be used 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: 01/12/09

Classified material must not be removed from official premises except when necessary in the conduct of official meetings, conferences, or consultations and must be returned 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 carry with them a Form AID 500-7, Courier Authorization Card **[Note: This form can be obtained by contacting SEC**].

USOs are responsible for issuing Courier Authorization Cards to designated personnel immediately after providing the appropriate security briefing. The designated courier

must sign an acknowledgement of responsibilities. USOs may issue Courier Authorization Cards for a maximum period of one year.

568.3.3.9 Reproduction of Classified

Effective Date: 01/12/09

Only the Top Secret Control Officer (TSCO) may reproduce Top Secret information. Reproduction must be performed on authorized equipment. The reproduction of Secret and Confidential information will be performed only on photocopy equipment specifically designated for the reproduction of classified material. The USO is responsible for posting the necessary signage to designated photocopy machines authorized for the reproduction of classified materials.

568.3.3.10 Destruction Procedures

Effective Date: 01/12/09

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/Administrative Services, Facilities Management Division (M/AS/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 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

Effective Date: 01/12/09

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: 01/12/09

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 affects 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

    1) the prospective recipient 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: 01/12/09

All new or re-employed Direct-Hire personnel, PSCs, and Purchase Order Contractors (Experts/Consultants) must attend or complete the Initial Security Briefing and sign the Form SF-312, Nondisclosure Agreement, at the time of their entrance on duty and prior to being afforded access to national security (classified) information [**Note: This form can be obtained by contacting SEC**]. 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: 01/12/09

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.

568.3.4.4 Unit Security Officer Training (USO)
Effective Date: 01/12/09

SEC provides training for new USOs. Each newly designated USO is required to attend such training within 90 days of their written appointment.

568.3.4.5 Special Access
Effective Date: 01/12/09

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

568.3.4.6 Termination Briefings
Effective Date: 01/12/09

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: This form can be obtained by contacting SEC**].

568.3.5 Security Incident Program
Effective Date: 01/12/09

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

Employees or contractors 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, and/or SEC. 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 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 HR, 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: 01/12/09

a. Employees or contractors must report all security incidents to SEC/CTIS/IS. 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/IS will investigate the incident and complete a Form OF 118, Record of Violation [**Note: This form can be obtained by contacting SEC**]. The security officer from SEC will forward the OF-118 to the person alleged to be responsible for the incident who will 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/IS 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 Cognizant Technical Officer.

568.3.5.2 Security Inspections

Effective Date: 01/12/09

Executive Order 12958 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, 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 has 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 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 security policies, or as part of an investigation for work-related misconduct.

Cleared U.S. citizen security personnel designated by SEC and/or cleared contract employees 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, ClassNets and secure telephones);
- Doors, alarms, and locking mechanisms;
- Access granted to visitors and employees;
- End-of-day check procedures;
- Destruction procedures; and
- Security training.

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.

568.3.5.3 Examples of Security Incidents

Effective Date: 01/12/09

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.

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 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.

568.3.5.4 Categorization of Security Incidents

Effective Date: 01/12/09

Security incidents are investigated and adjudicated as either a security infraction or violation, depending upon the classification level of the material in question and the degree of compromise to that material.

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.

568.3.5.5 Disciplinary Actions and Security Clearance Review Related to Security Infractions

Effective Date: 01/12/09

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 infraction, the SEC/CTIS/IS 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 infraction within 36 months, the SEC/CTIS 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 infraction within the 36-month window will result in the Deputy Director (DD) of SEC referring the matter to HR for possible disciplinary action and a concurrent review within SEC to determine the offender's continued eligibility to hold a security clearance.

568.3.5.6 Disciplinary Actions and Security Clearance Review Related to Security Violations

Effective Date: 01/12/09

a. Following an affirmative adjudication by SEC/CTIS/IS 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 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. HR may issue a letter of admonishment or reprimand, suspend the violator without pay, or terminate employment.

d. If the violator is a contractor or recipient employee or a Personal Services Contractor, SEC/CTIS/IS 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.

568.3.5.7 Appeals of Security Incidents

Effective Date: 01/12/09

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

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

- Upon receipt of the appeal, SEC/CTIS/IS will forward it to SEC/CTIS for a decision. An employee statement on Form OF-118, Record of Violation, does not initiate the appeal process [**Note: This form can be obtained by contacting SEC**].

568.3.5.8 Contractor Personnel Overseas
Effective Date: 01/12/09

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 SF-312, Classified Information Nondisclosure Agreement, when initially briefed [**Note: This form can be obtained by contacting SEC**].

- When access to classified information is no longer required, the person who no longer needs the access must sign the debriefing section of the form SF-312, and the USO must forward the SF-312 to SEC.

568.3.6 Processing National Security (Classified) USAID Automated Systems
Effective Date: 01/12/09

In USAID/Washington, Classified National Security Information must be processed on dedicated, stand-alone microprocessors approved to process such information or on a SEC-approved network (see the AMS Officer for locations of SEC-approved microprocessors).

The processing, storing, printing, or transmitting of classified information on any unauthorized network, distributed system, or mainframe 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: 01/12/09

ADS 569, Counterintelligence Program; **12 FAM 262, Security Awareness and Contact Reporting**; **12 FAM 263, Counterintelligence Awareness Program**; and **12 FAM 264, Personal Travel to Critical Human Intelligence Countries** contain the policy and procedures for the USAID counterintelligence program and implementation of PDD/NSC-12, Security Awareness and Reporting of Foreign Contacts.

568.4 MANDATORY REFERENCES
Effective Date: 01/12/09

568.4.1 External Mandatory References
Effective Date: 01/12/09

a. Director of Central Intelligence Directive 1/20, "Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)," of July 20, 1987

b. Executive Order (E.O.) 12829, "National Industrial Security Program," of January 6, 1993

c. E.O. 12958, "Classified National Security Information," March 28, 2003

d. E.O. 12968, "Access to Classified Information," of August 2, 1995

e. 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.)

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

g. 12 FAM 500, Information Security (This contains the policy and procedures for USAID implementation of E.O. 12958 concerning classified information.)

h. 12 FAM 557.1, Disciplinary Action for Security Violations in State, USAID, and OPIC

i. Marking Classified National Security Information, ISOO Publication

j. Information Security Oversight Office (ISOO) Directive Number 1, September 22, 2003

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

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

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

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

o. 5 U.S.C. 552b(1)

568.4.2 Internal Mandatory References

Effective Date: 01/12/09

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 569, Counterintelligence**

568.4.3 Mandatory Forms
Effective Date: 01/12/09

a. **AID 500-7, Courier Authorization Card [Note: This form can be obtained by contacting the Office of Security (SEC)]**

b. **OF-118, Record of Incident [Note: This form can be obtained by contacting SEC]**

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: This form can be obtained by contacting SEC]**

f. **SF-701, Activity Security Checklist [Note: This form can be obtained by contacting SEC]**

g. **SF-702, Security Container Check Sheet [Note: This form can be obtained by contacting SEC]**

h. **SF-703, Top Secret Cover Sheet [Note: This form can be obtained by contacting SEC]**

i. **SF-704, Secret Cover Sheet [Note: This form can be obtained by contacting SEC]**

j. **SF-705, Confidential Cover Sheet [Note: This form can be obtained by contacting SEC]**

568.5 ADDITIONAL HELP
Effective Date: 01/12/09

568.6 DEFINITIONS
Effective Date: 01/12/09

The terms and definitions listed below have been included into 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**, **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. (Chapters **562**, **568**)

Classified National Security Information (Classified Information)
Any data, file, paper, record, 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. 12958 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**)

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**)

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**)

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 e.g., 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. (Most security violations occur outside a controlled access area.) (Chapter **568**)

568_011209