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

Table of Contents

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

568.1 OVERVIEW

This ADS chapter provides the policy for USAID's implementation of Executive Orders (EO) 12958, 12968, and 12829, 12 FAM 500, and PDD/NSC-12 as they relate to information security programs, contact reporting, and counterintelligence awareness training.

568.2 PRIMARY RESPONSIBILITIES

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 EOs. **(See Mandatory References, EO 12958, EO 12968, and EO 12829).**

b. The Executive Secretary (ES) is responsible for establishing and maintaining a system of accounting for Top Secret documents and any special access programs in USAID in accordance with Section 4.4 of EO 12958. **(See Mandatory Reference, EO 12958)** Additionally, 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.

d. The Unit Security Officer is responsible for ensuring that all operations conducted by the Bureau, Mission, or work unit are carried out in conformance with the security regulations contained in Chapters 561 to 568 of this directives system.

568.3 POLICY AND PROCEDURES

568.3.1 National Security (Classified) Information Security

12 FAM 500 contains the policy and procedures for USAID and all foreign affairs agencies on the implementation of EO 12958. **(See Mandatory References, 12 FAM 500** and **EO 12958)**

The head of each Bureau, Independent Office, and overseas USAID Mission must appoint a Unit Security Officer.

USAID original classification authorities (OCA) must prepare classification guides covering the information for which they have program responsibility. Each classification guide must be approved personally and in writing by the OCA. The guides must

conform to the standards and directives issued under EO 12958 and are subject to review by the senior Agency official.

The number of USAID officials possessing original classification authority for National Security Information must be strictly limited.

The following positions in USAID have OCA authority to originally classify information at the Confidential and Secret level:

- Administrator (A/AID);
- Deputy Administrator (DA/AID);
- Chief of Staff;
- Executive Secretary (ES);
- Director of Security (D/SEC);
- Assistant Administrator for Policy and Program Coordination (AA/PPC);
- Assistant Administrator, Bureau for Africa (AA/AFR);
- Assistant Administrator, Bureau for Europe and Eurasia (AA/E&E);
- Assistant Administrator, Bureau for Latin America and the Caribbean (AA/LAC);
- Assistant Administrator, Bureau for Asia and the Near East (AA/ANE);
- Assistant Administrator, Bureau for Humanitarian Response (AA/BHR);
- Assistant Administrator, Bureau for Global Programs, Field Support and Research (AA/G);
- Assistant Administrator, Bureau for Management (AA/M);
- Director, Office of Administrative Services (M/AS/OD);
- Inspector General (IG);
- Deputy Inspector General (DIG);
- Senior Policy Advisor;

- Counselor.

568.3.1.1 Annual Summary Preparation

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. The summary must be provided to the Office of Security (SEC) at the conclusion of each fiscal year for inclusion in the Agency's annual report to the Information Security Oversight Office (ISOO).

568.3.1.2 SEC Review

At SEC's request, all classified documents originated within USAID must be made available to SEC for review for compliance with marking and classification requirements.

In USAID/Washington, all Bureaus and Independent Offices must maintain a centralized file containing a copy of all classified documents produced within their respective Bureau/Office. All USAID overseas offices must send SEC a copy of all the classified documents they produce within 30 days of preparation.

*568.3.1.3 Security Infractions and Violations

*The following section outlines the new security incident policy effective May 4, 2001.

- An employee or contractor who commits security infractions or violations, or a supervisor who fails to provide effective organizational security procedures, may be subject to administrative, disciplinary, or security clearance actions initiated as appropriate by the Office of Human Resources (HR), the contracting office, or SEC.

- Disciplinary and 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 Infraction and Violations program, SEC will maintain files on all personnel who have incurred security infractions or security violations. Deliberate or excessive 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.

- The same security infraction/violation can be considered more than once, if it occurs within the 36-month window. People currently charged with security incidents under the previously employed 18-month policy remain subject to that policy until their 18-month window expires.

- All new security incidents that occur after May 4, 2001 will be counted under the new policy.

*568.3.1.4 Disciplinary Actions and Security Clearance Review Related to Security Infractions

*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 Chief of the Office of Security, Personnel, Information, and Domestic Security Division, Information and Domestic Security Team (SEC/PIDS/IDS) will send a letter of warning to the offender. The offender is required to send a signed reply acknowledging that he or she understands the policies and ramifications of future security incidents. The offender will also be required to attend a security refresher briefing as directed by SEC.

*c. For a second infraction within 36 months, the SEC/PIDS Chief will send the offender a letter that includes a statement concerning the actions SEC and HR 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 another security refresher briefing.

*d. A third or subsequent infraction within the 36-month window will result in the Deputy Director 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.

*568.3.1.5 Disciplinary Actions and Security Clearance Review Related to Security Violations

*a. Following an affirmative adjudication by SEC/PIDS/IDS that a security violation has occurred, SEC/PIDS 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/PIDS 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.

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

*568.3.1.6 Appeals of Security Incidents

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

- The appeal must be dated within 30 days of notification from SEC/PIDS/IDS of the decision to assign responsibility for the incident.

- On receiving the appeal, SEC/PIDS/IDS will forward it to SEC/PIDS for a decision. An employee statement on Form OF-118, Record of Violation, does not initiate the appeal process.

568.3.1.7 Contractor Personnel Overseas

Overseas, the USAID Mission Unit Security Officer 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 security briefing and debriefing to ensure that they understand security requirements.

- All contractor personnel must sign the SF-312, Classified Information Nondisclosure Agreement, when initially briefed. **(See Mandatory References, 12 FAM 564.1, Initial Briefings, and SF-312)**

- When access to classified information is no longer required, the debriefing section of the form SF-312 must be signed by the person who no longer needs the access and forwarded to SEC.

*568.3.2 Processing National Security (Classified) and Sensitive But Unclassified (SBU) Information on USAID Automated Systems

*In USAID/W, Classified National Security Information must be processed on dedicated stand-alone microprocessors approved to process such information or on a SEC-approved network (see AMS Officer for location 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. (See Mandatory Reference, ADS 552)**

- USAID Sensitive But Unclassified (SBU) information is unclassified and warrants a degree of protection and administrative control based on the originator's determination.

568.3.3 Counterintelligence

12 FAM 262, Security Awareness and Contact Reporting, and 264, Counterintelligence Awareness Program, contain the policy and procedures for the USAID counterintelligence program and implementation of PDD/NSC-12, Security Awareness and Reporting of Foreign Contacts. **(See Mandatory References, 12 FAM 262 and 264)**

568.4 MANDATORY REFERENCES

568.4.1 External Mandatory References

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 (EO) 12829, "National Industrial Security Program," of January 6, 1993**

c. **EO 12958, "Classified National Security Information," of April 17, 1995**

d. **EO 12968, "Access to Classified Information," of August 2, 1995**

e. **12 FAM 262, Security Awareness and Contact Reporting, and 264, 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 500, Information Security** (This contains the policy and procedures for USAID implementation of EO 12958 concerning classified information.)

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

h. **12 FAM 564.1, Initial Briefings**

i. **12 FAM 769, Personal Travel to Critical Human Intelligence Threat Countries, September 15, 1991**

j. **Information Security Oversight Office (ISOO) Directive Number 1, of October 13, 1995**

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. **SF-312, Classified Information Nondisclosure Agreement**

568.4.2 Internal Mandatory References

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**

568.5 ADDITIONAL HELP

***568.6 DEFINITIONS**

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 information
See the definition for classified national security information. (Chapters 562, 566, 567, and 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 EO 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, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs. (Chapters 562, 568)

marking
The physical act of indicating on national security information the proper classification levels, the classification authority, the Agency and office of origin, declassification and downgrading instructions, and special markings which limit the use of the classified information. (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_071001_w091003