Functional Series 500 - Management Services
Chapter 552 - Classified Information Systems Security

Table of Contents

552.1 OVERVIEW 3

552.2 PRIMARY RESPONSIBILITIES 4

552.3 POLICY AND PROCEDURES 5

552.3.1 Classified Information Systems (IS) Protection 5
552.3.1.1 Information Systems Security (ISS) Program 6
552.3.1.2 Access to Classified IS 6

552.3.2 Classified Information Processing 7
552.3.2.1 Classified Information Processing - Overseas 8
552.3.2.2 Classified Information Processing – USAID/Washington 8

552.3.3 Personnel Requirements 8
552.3.3.1 Security Clearances 9
552.3.3.2 Personnel Management 9

552.3.4 Technical Security 10
552.3.4.1 Additional Technical Security Requirements 10
552.3.4.2 Security Incident Reporting 10

552.3.5 Administrative Security 11
552.3.5.1 Appointment of ISSOs and Alternates, and User Approval 11
552.3.5.2 Access to Computer Systems Approved to Process Classified Information 12
552.3.5.3 Use of Systems Approved to Process Classified Information 12
552.3.5.4 Protecting Information Displayed and Processed on Classified Systems 12
552.3.5.5 Violations 15
552.3.5.6 System Maintenance 15
552.3.5.7 Record Keeping 16
552.3.5.8 Security Reviews 16
552.3.5.9 Training 17
552.3.5.10 Backup, Emergency Action, and Contingency Operations Planning 18
552.3.5.11 System Certification 18

552.3.6 Physical Security 18
552.3.6.1 Additional Details on Physical Security 19
552.3.6.2 Physical Security Issues in Emergency Action and Contingency Operation Planning 20

552.3.7 Host Facility System Security Standards 20

552.3.8 Secure Telephone Units (STU-III) or Secure Telephone Equipment (STE), and Their Connection to Fax Equipment 21
552.3.8.1 Procurement of STU III/STE 21
552.3.8.2 Installation and Repair of STU-III/STE and Secure Fax Equipment 21
552.3.8.3 Transmissions on STU-III/STE 22
552.3.8.4 Administrative Management of STU-III/STE 22

552.4 MANDATORY REFERENCES 23

***552.4.1 External Mandatory References 23**

552.4.2 Internal Mandatory References 25

552.5 ADDITIONAL HELP 26

552.6 DEFINITIONS 27

Functional Series 500 - Management Services
Chapter 552 - Classified Information Systems Security

552.1 OVERVIEW

This chapter outlines the basic policies that underlie the Agency's Classified Information Systems (IS) Security Program.

Note: The former term, "Automated Information Systems" has been replaced by "Information Systems" throughout this chapter.

- USAID overseas people and organizations that process classified data must comply with the Department of State's Foreign Affairs Handbook, 12 FAH-6 (OSPB Security Standards and Policy Handbook). Overseas, classified data processing, classified telephone discussions and classified or sensitive fax transmissions, are authorized only within U.S. Embassies on equipment approved for such use by the appropriate authorities, in approved areas. Some missions have Secure Telephone Units (STU-III) that are used to transmit Sensitive But Unclassified (SBU) data. Those missions must comply with paragraph 552.3.8 of this chapter.

- USAID Washington (USAID/W) people and partners that process classified data on stand-alone computers must comply with ADS 552. Some forms, formats, and guidance in ADS 545, Information Systems Security, also apply to classified USAID IS.

The guidance in this chapter only applies to use of USAID/W **information technology (IT) and** computer systems approved to process information classified at the SECRET or CONFIDENTIAL level. **Personal use of Agency information systems approved to process classified information is prohibited. Also, you *MUST NOT* use personal electronic equipment or devices to process classified data**.

This chapter contains the following:

- USAID'S overall policies and procedures to protect classified IS;

- General IS access procedures (personnel, technical, and administrative security requirements for classified information processing);

- Selected procedures for access to and processing classified data; and

- Details on USAID classified facsimile and communications security requirements.

552.2 PRIMARY RESPONSIBILITIES

Law and Federal guidance require agencies to incorporate security into their information technology architectures and the life cycles of their information systems. More detailed security responsibilities apply to Mission Critical Systems and National Security Systems (see 552.6, Definitions, for statutory and regulatory terms that apply to information systems). Within USAID, primary information systems security responsibilities are as follows:

a. The Administrator is responsible for developing and implementing a comprehensive, Agency-wide Information Systems Security (ISS) program that is technically current, cost effective, and in full compliance with established national security directives. The Administrator has delegated this responsibility to the Bureau for Management, Office of Information Resources Management (M/IRM). More details on Agency IS security responsibilities are contained in the Internal Mandatory Reference, "Information Technology Security Roles and Responsibilities."

b. The **Deputy** Assistant Administrator, Bureau for Management (AA/M) serves as the Chief Information Officer (CIO). The CIO is responsible for directing, managing, and providing policy guidance and oversight with respect to all Agency information resource management activities. These responsibilities may be delegated to senior-level office managers. USAID's Information Systems Security Officer (USAID ISSO), program managers, designated site ISSOs, and information technology (IT) systems managers carry out USAID security management activities.

c. The Bureau for Management, Office of Information Resources Management (M/IRM) is responsible for providing "signatory approval to operate" for all information systems used to process, store, or print sensitive but unclassified information. The Director of M/IRM has the authority to approve, subsequent to coordination with the Director of the Office of Security (D/SEC), the use of all information systems used to process, store, or print classified national security information. The Director of M/IRM also has been assigned responsibility for compliance with federal regulations related to Communications Security (COMSEC), and operational security for secure telecommunications devices with associated cryptographic equipment. M/IRM also fulfils other USAID **IT and** IS-related functions.

d. The ISSO for USAID is designated by the Administrator and is directly responsible for overseeing and executing the bulk of the Agency's operational information systems security activities. **In addition, USAID's ISSO, in conjunction with the Office of the Inspector General (IG) and the Office of Security (SEC), will develop and implement methodologies for:**

- **Detecting, reporting, and responding to IS security incidents;**
- **Notifying and consulting with law enforcement officials about IS security incidents;**

- **Notifying and consulting with other offices and authorities, to include the General Services Administration's Federal Computer Incident Response Capability (FedCIRC) in the event that a significant IS security incident occurs.**

e. The Director, Office of Security (D/SEC) **is responsible for**

- **Providing clearance certification for access to systems;**

- **Inspecting classified systems to determine system operations and use comply with established policies and applicable Federal security guidelines; and**

- **Providing technical guidance and security policy determinations.**

f. The Office of the Inspector General (IG), consistent with legal and regulatory guidance, will conduct annual evaluations of USAID information systems.

g. Designated site ISSOs within USAID organizations, IT Specialists (USAID/W), System Managers (USAID Missions), IT system staff, and users **also** have responsibilities for IS security functions. Individual users are responsible for

- **Using classified systems for official business purposes only;**

- **Complying with existing system operating guidance; and**

- **Reporting known or perceived problems that could impact system availability or the integrity of the data being created and stored.**

552.3 POLICY AND PROCEDURES

The statements contained in section .3 of this ADS chapter are the official Agency policies and procedures that implement official Agency information systems security policies.

552.3.1 Classified Information Systems (IS) Protection

It is the policy of USAID to protect the Agency's classified electronic information commensurate with the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of such information. All data of value to the Agency requires some minimum level of protection. Certain data, because of the sensitivity or criticality of the information to the mission of USAID, requires additional safeguards. Failure to protect Classified National Security Information (Classified

Information) can lead to adverse administrative actions, and both civil and criminal penalties.

The Agency's policy is to implement and maintain an Information Systems Security (ISS) program to ensure that adequate computer security is provided to all Agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. All USAID networked computer systems **(used to process unclassified data)** and stand-alone terminals used to process classified data must provide controlled access protection safeguards to protect the integrity, availability, and where required, confidentiality of Agency information.

552.3.1.1 Information Systems Security (ISS) Program

USAID's ISS Program implements policies, standards, and procedures that are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget (OMB), the Department of Commerce (DOC), the General Services Administration (GSA), the Department of Defense (DoD), the Department of State (DOS), the Information Security Oversight Office (ISOO), and the Office of Personnel Management (OPM). Different or more stringent requirements for securing national security information will be incorporated into USAID classified programs as required by appropriate national security directives. Classified processing requirements do not apply to unclassified systems. However, at a minimum, USAID's ISS program requires that the controls outlined in OMB A-130, Appendix III must be implemented in all Agency general support and major applications systems. **(See External Mandatory Reference, OMB Circular A-130, Appendix III)**

552.3.1.2 Access to Classified IS

a. USAID's security policy for access to classified USAID computer systems is designed to protect classified national security information against unauthorized access or disclosure. Before granting access to any IS approved for processing classified data, you must verify the individual has the appropriate level security clearance. To implement this policy, USAID uses formal authorized access permission procedures that are based on a clearly demonstrated need to know or need to use determination for every person granted access to a USAID IS that processes classified data. USAID's security policy is supported by an approved personnel screening process and formal authorization approval. When all these factors are used together, they implement the USAID security policy for USAID classified system access.

- Agency people and partners seeking to gain access to classified IS for new USAID direct-hire employees or contractors must submit the AID Form 6-1 (Request for Security Action) to SEC.

- SEC will provide an AID Form 500-3 (Security Investigation and Clearance Record) to advise the entity that requested a personal background investigation and/or security clearance action of their determination.

- If a new person requires access to the Ronald Reagan Building, an AID Form 500-1 (Request for Issue (Reissue) of Building Pass) will also need to be submitted to SEC.

NOTE: AID Forms 500-1, 500-3 and 6-1 are only available on the USAID intranet web site at http://inside.usaid.gov/forms/.

b. Authorization to work full time, or on a random, re-occurring basis in the USAID headquarters building is contingent on a background investigation and a favorable review by SEC. Upon the favorable review and sponsorship by a USAID Bureau/Office, a permanent USAID Headquarters Building Pass may be issued.

c. Visitor passes are issued in accordance with the procedures outlined in ADS 565, paragraph 565.3.4. Visitor passes require escort, and are intended for the non-business guests of employees or official participants at occasional meetings, where upon completion of the business, the visitor departs. Visitor passes will not be issued in lieu of compliance with the paragraph above.

552.3.2 Classified Information Processing

All personnel with information systems security (ISS) responsibilities must adhere to the following personnel, technical, administrative, and physical security policies and procedures when USAID equipment is used to support Agency objectives.

- **Personnel Security:** The personnel security aspects of ISS require determinations that an individual's personal reliability and trustworthiness meet specified criteria, and identification of a need to know and access particular types of data to perform assigned functions.

- **Technical Security:** The technical security aspects of ISS require implementation of technological methodologies to ensure that data is accessible, verifiable, and secure from unauthorized access or damage.

- **Administrative Security:** The administrative security aspects of ISS require documentation of critical security actions as they are completed to demonstrate compliance.

- **Physical Security:** The physical security aspects of ISS protect hardware, software, and other IS components from damage or loss (including loss due to negligence or intentional misconduct).

552.3.2.1 Classified Information Processing - Overseas

The requirements for processing Classified National Security Information overseas are contained in 12 Foreign Affairs Handbook 6 (12 FAH-6), OSPB Security Standards and Policy Handbook. Overseas, classified data processing is authorized only within U.S. Embassies on equipment approved for such use by the appropriate authorities. **If a USAID Mission overseas has a need to process classified data outside the U.S. Embassy, the Mission Director must submit written justification (including an endorsement from the Department of State Regional Security Officer, RSO) to SEC and M/IRM.**

See also ADS 562, Physical Security Programs (Overseas) and External Mandatory References 12 Foreign Affairs Manual (FAM) 630, Classified Automated Information Systems and 12 FAM 640, Domestic and Overseas Automated Information Systems Connectivity.

552.3.2.2 Classified Information Processing – USAID/Washington

Classified National Security Information will only be processed within Restricted Areas. Equipment used for such processing must not be removed from the Restricted Area without coordination with M/IRM, SEC, and the ISSO. **(See also ADS 562, Physical Security Programs (Overseas) and ADS 565, Physical Security Programs (Domestic))**

a. Program Managers, IT Specialists, supervisory personnel, and end-users who have responsibilities, duties, or tasks in support of USAID must adhere to the following personnel, technical, administrative, and physical security policies when equipment approved to process classified information is used to support program activities and mission objectives. **(Additional details can be found in ADS 561, Security Responsibilities, ADS 566, U.S. Direct-Hire and PASA/RSSA Personnel Security Program, ADS 567, Classified Contracts, Grants, Cooperative Agreements, and Contractor/Recipient Personnel Security, and ADS 568, National Security Information and Counterintelligence Security Program.)**

b. The Office of Security (SEC) conducts background investigations on USAID direct hires. Because the Defense Security Service (DSS) conducts background investigations on USAID institutional contractors, and is also responsible for oversight of contractor facilities where classified data is stored and/or processed, some applicable security policies and procedures can be found in 32 Code of Federal Regulations (CFR) Part 154, Department of Defense Personnel Security Program Regulation, and Department of Defense Manual DoD 5220.22-M, National Security Program Operating Manual. **(See 32 CFR 154 and DoD Manual 5220.22-M)** Additional specifics on Defense-related security requirements can be found in the Additional Help "Selected Security Guidance." **(See Additional Help, Selected Security Guidance)**

552.3.3 Personnel Requirements

552.3.3.1 Security Clearances

All personnel accessing USAID classified information systems must have the following:

- A security clearance commensurate with the highest classification of information ever processed or stored on the system;
- The appropriate access levels;
- A need-to-know in connection with the performance of official duties; and
- Knowledge of their computer security responsibilities.

(See also ADS 561, Security Responsibilities, ADS 566, U.S. Direct-Hire and PASA /RSSA Personnel Security Program, ADS 567, Classified Contracts, Grants, Cooperative Agreements, and Contractor/Recipient Personnel Security)

552.3.3.2 Personnel Management

a. Responsible supervisors must ensure that a statement establishing responsibilities for classified information systems security is included in position descriptions for the ISSO for USAID, designated site ISSOs, IT Specialists, members of system staffs, Program Managers, System Managers, and any other personnel having a direct responsibility for safeguarding Agency computer systems. Human Resources Personnel Operations Division (M/HR/POD) staff are available to assist supervisors in the development of position descriptions.

b. Visitors, custodial, and facility maintenance personnel who are inside restricted areas and do not have security clearances must be escorted and kept under continuous observation by personnel who are authorized unescorted access to those areas.

(1) The procedures for requesting security clearances are contained in ADS 566, U.S. Direct-Hire and PASA/RSSA Personnel Security Program and ADS 567, Classified Contract Security and Contractor Personnel Security Program. **(See ADS 566 and ADS 567)**

(2) The IT Specialist must ensure that all vendor maintenance and customer support personnel are cleared at a level commensurate with the highest classification of information authorized to be processed on the equipment. All the requirements specified in paragraph 552.3.3.1 apply to vendor maintenance and customer support personnel who may access classified data in the course of their activities. **(See 552.3.3.1)**

552.3.4 Technical Security

USAID Bureaus/Offices must control access to specialized system software, utilities, and functionalities that could be used to gain unauthorized access to application data and program code. Classified information systems must be operated in accordance with the following policies:

- Classified information must be processed on dedicated, stand-alone computer systems approved by SEC to process such information. The processing, storing, printing, or transmitting of classified information on any USAID-owned network, distributed system, or mainframe computer system is strictly prohibited. Exemptions to this policy must be approved by M/IRM. **(See ADS 568, National Security Information and Counterintelligence Security Program)**

- Users must not install personally owned software, shareware, or freeware on classified systems owned or operated by the Agency.

- Users must not install or use personally owned computers, communication devices, printers, or other peripheral computing devices in facilities housing computer systems approved to process classified information without written approval from the Agency ISSO. (**See ADS 550, End-User Applications)**

- All operating system and application software must reside on removable drives.

552.3.4.1 Additional Technical Security Requirements

a. Computer systems approved to process classified information must not be connected to any other information system.

b. Within USAID/W facilities, a 1-meter (39.37-inch) separation must be maintained between computer systems and printers approved to process classified information and other electronic and telephonic equipment. Contact M/IRM and SEC for assistance in determining what equipment is most appropriate for your organization's classified data processing requirements.

552.3.4.2 Security Incident Reporting

a. System managers and users who discover (or suspect) incidents of fraud, misuse, disclosure of information, destruction or modification of data, or unauthorized access attempts must immediately report such incidents to the designated site ISSO and Program Manager (USAID/W) or the USAID Executive Officer (EXO) (USAID Missions). **Anyone who discovers indications there may have been unauthorized**

access to, or abuse of, a classified system, or a possible compromise of Classified National Security Information, must contact SEC immediately.

b. Violations

(1) System users must not originate, process, print, or store classified information on any computer system not approved for that purpose. Individuals violating this provision will be subject to the security violation procedures set forth in ADS 568, National Security Information and Counterintelligence Security Program. **(See ADS 568) Investigations of possible compromise of Classified National Security Information on an automated system will be conducted by SEC or Unit Security Officer with assistance from M/IRM as appropriate.**

(2) Passwords to classified systems and sensitive data must be protected at the same level as the information being protected on the classified/sensitive system. Employees disclosing passwords to classified systems are subject to administrative sanctions or disciplinary actions.

(3) Program Managers, designated site ISSOs, and EXOs must take appropriate action to ensure that USAID personnel, contractors, and vendors meet technical security requirements for classified computer systems.

552.3.5 Administrative Security

Access to information systems approved to process classified information must be restricted to individuals requiring such access to perform their official duties. The level of access granted must limit users to only the information needed to complete their assigned responsibilities. The following policies must be followed to facilitate access controls. **(See ADS 568, National Security Information and Counterintelligence Security Program)**

552.3.5.1 Appointment of ISSOs and Alternates, and User Approval

a. The Administrator or the CIO must designate, in writing, an Agency employee to serve as the ISSO for USAID. The designee must have a TOP SECRET security clearance and be a U.S. citizen direct-hire employee.

b. Program Managers must appoint, in writing, a designated site ISSO and an alternate to manage the ISS Program for their organization. An appointment letter must be sent to the ISSO for USAID. Both designees must be U.S. citizen direct-hire employees of the Agency and have at least a SECRET security clearance.

c. Users approved by the designated site ISSO to process classified information must sign and complete a USAID Classified Information System Users Agreement. **(See Internal Mandatory Reference, USAID Classified Information System User**

Agreement, AID Form 552-2) Each completed copy of this form must be retained for six months after the individual it pertains to has left the Agency. Foreign nationals ***CANNOT*** be given authorization to process or access classified information.

552.3.5.2 Access to Computer Systems Approved to Process Classified Information

a. Program Managers must determine who within their organizational entity requires access to computers approved to process classified information. This determination must be in writing and based on a valid need-to-know. **(See Additional Help, Approval to Access and Process Classified National Security Information via Information Systems)**

b. Prior to receiving authorization to process classified information, the user must receive classified information processing and handling instructions from either the ISSO for USAID or the designated site ISSO.

c. Foreign nationals are not authorized to process or access classified information.

d. The entity IT Specialist/System Manager must maintain a visitors log **(AID Form 545-6)** for all properly cleared persons not normally assigned to an area where classified data processing is taking place. Prior to being allowed access to any area where there are systems approved for processing classified data, individuals not on the Authorized Access List **(AID Form 545-2)** must sign the Visitors Log.

e. Visitors must be kept under continuous visual observation by a person with authorized unescorted access. **(See Internal Mandatory References, Authorized Access List, AID 545-2, and Visitors Log, AID 545-6)**

552.3.5.3 Use of Systems Approved to Process Classified Information

Remember, the guidance in this chapter only applies to use of USAID computer systems approved to process information classified at the SECRET or CONFIDENTIAL level. Additional guidance on processing data that is classified TOP SECRET or that requires special handling (e.g., compartmented data or special access program data) is available from the Office of Security. **Personal use of Agency information systems approved to process classified information is prohibited**. **Also, you *MUST NOT* use personal electronic equipment or devices to process classified data**.

552.3.5.4 Protecting Information Displayed and Processed on Classified Systems

All users must ensure that no classified information is displayed on a screen when unauthorized or uncleared individuals are physically in a position to view the screen. The designated site ISSO must ensure that workstations located in high access areas or those exposed to potential public viewing are equipped with screens that restrict the

angle of viewing. Workstation screens must face away from windows and open access areas to prevent casual viewing of screens by unauthorized or uncleared individuals. Monitor and/or video screens displaying classified information must be protected in the same manner as other classified material or other classified equipment. **(See ADS 568)**

a. Removable data storage media (e.g., floppy disks, removable hard disks, tape drives, etc.) containing classified information must not be left unsecured or resident in a computer system when the computer system is unattended by personnel authorized to process classified information. All media containing classified material must be properly marked.

b. Users must ensure that classified files are not stored in a printer's queue or spool file, and printed classified information is not left unattended in a printer.

c. Labels indicating the highest classification level of information approved for processing on the system must be affixed to all computer devices and removable media. **(See ADS 568 and 12 FAM 500, Information Security)**

(1) The designated site ISSO must ensure that each device associated with a computer system approved to process, store, or print classified information is prominently labeled to indicate the highest classification level of information approved for the system.

(2) In addition to displaying the highest classification level of information approved for the system, classified system device labels must also indicate the name and phone number of the designated site ISSO responsible for the security of that piece of equipment.

(3) Users must affix labels to all removable media (i.e., floppy disks, removable hard disks, etc.) indicating the highest level of information approved for processing on the system.

(4) Labels for removable media indicating the highest level of information approved for processing on the system are ordered from GSA (FEDSTRIP) using the following National Stock Numbers:

- SECRET Label (SF) 707 7540-01-207-5537
- CONFIDENTIAL Label (SF) 708 7540-01-207-5538
- UNCLASSIFIED Label (SF) 710 7540-01-207-5539.

d. Documents, files, or records containing classified information must not be initially processed on unclassified systems then subsequently labeled or marked

as classified data. The following section describes how unclassified data may be transferred to a classified system.

(1) If you must move unclassified data to a classified stand-alone computer (to merge information into a classified document, for example) you can use a 3 1/4 inch floppy disk. This procedure is authorized for moving unclassified data from an unclassified computer to a computer approved for processing CONFIDENTIAL or SECRET data **ONLY**. You will need a previously unused, virus-scanned, blank disk for each transfer.

(2) Mark the blank disk with the appropriate classification level -- use the same classification level as the classified computer to which you are transferring the unclassified data, and copy the unclassified data onto the disk.

(3) Put the properly labeled transfer disk into the classified computer, and copy the unclassified data onto the classified system.

(4) If you insert a floppy disk into a classified computer, you must mark (and handle) the disk as classified at the same level as the computer where you used the disk. When the disk is no longer needed, you must destroy it.

(5) You may also use a CD-ROM (compact disk read-only media) prepared on an unclassified computer to transfer unclassified data to a classified computer, IF the CD drive on the classified computer is READ ONLY (not Read/Write).

REMEMBER you *CANNOT* transfer data generated on a classified computer to an unclassified computer, even if the text itself is unclassified.

e. Protection of Media and Output. Documentation and removable media (e.g., floppy disks, removable hard disks, etc.) must be stored in an approved security container.

(1) The Program Manager, designated site ISSOs, and users must ensure that all media used to produce classified hard-copy materials are protected in accordance with ADS 562, Physical Security Programs (Overseas), ADS 568 National Security Information and Counterintelligence Security Program, and the policies provided in this chapter. **(See ADS 562 and ADS 568)**

(2) The designated site ISSO or the ISSO for USAID must inform users of their duties in protecting classified media and hard-copy output. **(See ADS 561, Security Responsibilities)**

f. Destruction of Classified Media and Output. Destruction of removable media and classified output must be carried out by cleared U.S. citizens and accomplished by shredding or placing the material in a separate burn bag marked "Electronic Media."

552.3.5.5 Violations

a. The Office of Security (SEC) will investigate all suspected or known security incidents involving classified data and violations involving information systems that contain, or have contained, classified data. **(See ADS 568, National Security Information and Counterintelligence Security Program)**

b. Designated site ISSOs **must** randomly review selected storage media and system hardware associated with information systems under their purview to ensure that users are not processing information classified above the level authorized for the system, and that classified information is not being processed on unauthorized system equipment.

552.3.5.6 System Maintenance

a. Personnel who perform system maintenance must have a security clearance commensurate with the highest level of information approved for processing on the computer system**. (See ADS 566, U.S. Direct-Hire and PASA/RSSA Personnel Security Program and ADS 567, Classified Contracts, Grants, Cooperative Agreements, and Contractor/Recipient Personnel Security)**

b. The designated site ISSO must maintain a log of all maintenance service performed on information system equipment approved to process classified information.

c. Classified information systems maintenance logs must include the following information:

- Date of service;
- Service performed;
- Hardware or software involved;
- Name(s) of individual(s) performing the service;
- Equipment removed or replaced; and
- System condition or status following the service.

All maintenance log records must be retained in the central system file for a period of six months after the date of entry.

d. A suitably cleared and knowledgeable person must supervise vendor maintenance personnel when they access computer systems approved to process classified information and ensure that maintenance personnel do not remove any

storage media that have ever been used in conjunction with system equipment approved to process classified information.

e. Only personnel who are U.S. citizens with the appropriate level security clearance and M/IRM authorization are allowed to maintain TEMPEST equipment.

f. Maintenance personnel must not remove from Agency premises any hardware, software, or magnetic media that has been used in association with computer systems approved to process classified information without the expressed written permission of the designated site ISSO.

552.3.5.7 Record Keeping

The designated site ISSO must ensure that the original IS security documents, logs, and records listed below are maintained, after processing, in a central file for each system authorized to process classified information:

- Classified Information System User Agreement **(AID Form 552-2)** and Termination Notices;
- Contingency Operation, Disaster Recovery, and Emergency Action Plans;
- Copies of Waivers or Exceptions;
- System Certification Documentation;
- System Maintenance Logs;
- Security Reviews;
- Designated site ISSO and Alternate Appointment Documentation;
- Annual Classified Processing Compliance Reviews **(AID Form 552-1)**; and
- System Inventories.

Blank copies of forms and examples for the development and completion of many of these IS security documents, logs, and records are provided in the Internal Mandatory References and Additional Help sections of this chapter.

552.3.5.8 Security Reviews

The Annual Classified Processing Compliance Review must address personnel, administrative, technical, and physical security practices. **(See Internal Mandatory Reference, Classified Processing Compliance Review, AID Form 552-1)** The

results of the review must be retained in the central system file with a copy forwarded to the ISSO for USAID annually. This evaluation must result in a draft report with findings and recommendations for the ISSO for USAID. The final report must be distributed to the Program Manager, the appropriate office director, M/IRM, and SEC.

The results of a Classified Processing Compliance Review, that may identify USAID vulnerabilities, must be appropriately marked for those with a need to know (e.g., banner the top of each page "Release Restricted-Verify Need to Know Before Permitting Access") in addition to other administrative markings (such as Sensitive Unclassified Information, CONFIDENTIAL, SECRET, TOP SECRET, NOFORN, NOCONTRACT, etc.) appropriate to the content of the document. Additional information on Sensitive But Unclassified (SBU) Information can be found in 12 FAM 540. **(See 12 FAM 540, Sensitive But Unclassified Information)**

a. The designated site ISSO must ensure that computer systems approved to process classified information are installed in accordance with the National COMSEC Information Memorandum (NACSIM 5203), "Guidelines for Facility Design and RED/BLACK Installation," available from the USAID COMSEC Office.

b. The designated site ISSO, in conjunction with the Program Manager and other appropriate Agency personnel, must conduct an annual review of user and information systems operating practices to evaluate compliance with Agency security policies.

c. The ISSO for USAID must conduct or direct the performance of security evaluations of computer systems authorized to process classified information when significant modifications are made to the system; or, if no significant modifications are made to the system, at a minimum once every three years. These evaluations must address compliance with applicable Federal and Agency information systems security policies, standards, and requirements.

552.3.5.9 Training

a. The ISSO for USAID must provide security training to designated site ISSOs, Program Managers, and users authorized to process classified information. Upon request, the ISSO for USAID must provide special training for other Agency personnel who have security responsibilities for Agency classified systems.

b. The designated site ISSO must ensure that annual computer security awareness training is provided to all USAID classified system users. The designated site ISSO must ensure that personnel who have not had initial security awareness training are not permitted access to systems authorized to process classified information. Also, the designated site ISSO must ensure that annual security awareness training is provided to all classified system users.

c. The Agency ISSO and the designated site ISSOs must provide annual training in Washington or at the missions to address application-specific security measures.

552.3.5.10 Backup, Emergency Action, and Contingency Operations Planning

Program Managers and the designated site ISSO must develop, test, and implement emergency action plans for each facility accommodating an information system approved to process classified information. Emergency action plans must be coordinated with the ISSO for USAID and be consistent with applicable Agency and local government emergency action plans. **(See also ADS 545, Information Systems Security, ADS 530, Emergency Planning Overseas, and ADS 531, Continuity of Operations Program)**

a. Program Managers and designated site ISSOs must review, update (if necessary), and test all emergency action plans annually or when significant modifications are made to system hardware, software, or system personnel.

b. The designated site ISSO must retain copies of the most recent emergency action and contingency operation plans in the system's central file and at a backup site.

c. The designated site ISSO must develop site-specific Disaster Recovery Plans based on threat identification information, system resource accounting, and criticality assessment data.

d. Users must backup all files retained on properly marked removable media, and ensure that such media are secured in approved security containers when not in use.

552.3.5.11 System Certification

No classified data can be processed using computer systems unless the system has been accredited by the appropriate approving authority. **(See Additional Help, Information System Certification and Approval to Operate)**

552.3.6 Physical Security

Users must follow the policies in this paragraph to ensure that classified information systems are afforded the physical protection required for the highest classification level and most restrictive category of data or information stored or processed on the system. **(See ADS 562, Physical Security Programs (Overseas) and ADS 565, Physical Security Programs (Domestic))**

a. In USAID/W, computer systems approved to process classified information must only be located in Restricted Areas. **(See ADS 562 and 565)**

b. The IT Specialist and designated site ISSO must maintain a complete and up-to-date inventory of all system components and peripheral system devices at their location.

c. At the end of each business day, the designated site ISSO must conduct or direct the performance of an end-of-day security check of all work areas housing computer systems approved to process, store, or print classified information.

d. Laptop computers without removable hard drives that are authorized to process classified information must be transported and stored in the same manner as classified information. For those laptops with removable hard drives that contain classified data, the removable drives must be transported and stored in the same manner as classified information.

e. The Office of Security must assist the requesting Bureau, Office, or Mission by providing requirements for security measures. **(See ADS 568)**

552.3.6.1 Additional Details on Physical Security

a. Use of Computers for Processing Classified Data.

(1) Personnel with access to computer systems owned or operated by USAID must protect USAID information, equipment, and facilities**. This is especially important for computer systems used to process classified data.** Action will be taken against violators as stated in ADS 568, National Security Information and Counterintelligence Security Program. **(See ADS 568)**

(2) You may only enter classified information onto systems approved for processing such information. The creation, processing, or storage of classified information on systems not approved for such purposes is a security violation as defined in ADS 568, National Security Information and Counterintelligence Security Program. The limitations against retroactively classifying data also apply to documents prepared on information system equipment. **(See ADS 568)**

(3) The designated site ISSO must advise all system users to use the most stringent access controls available (e.g., generate data on a floppy disk using a stand-alone microcomputer) when processing classified information. Storage of such information on USAID distributed or networked systems is ***PROHIBITED***. More details on classified information can be found in 12 FAM 090, Definitions of Diplomatic Security Terms. Also, the information systems security practices included in ADS 545 must be applied to classified information systems to the extent they are practicable. **(See Mandatory References, 12 FAM 090, Definitions of Diplomatic Security Terms and 12 FAM 550, Security Infractions, Violations, and Unauthorized Disclosures)**

b. Monitoring System Users. The designated site ISSO must conduct reviews of randomly selected user word-processing documents, files, and floppy disks on a monthly basis to ensure that users are adequately protecting classified information.

552.3.6.2 Physical Security Issues in Emergency Action and Contingency Operation Planning

a. USAID/W Secure Facilities: M/IRM/TCO, in consultation with the Office of Security and the appropriate Program Managers, must identify and secure, through a contractual agreement, facilities to store backup classified data and/or media to ensure continuity of operations for systems operating in USAID/W. Such facilities must be off-site and employ appropriate environmental controls and alarm systems.

b. Mission Secure Facilities: At mission locations, the System Manager, in consultation with the EXO, must identify a secure location to store backup classified data and media to ensure continuity of operations for all computers and computer peripherals used to process classified data for which the System Manager is responsible.

c. USAID/W Emergency Action Plans: The IT Specialist/System Manager and designated site ISSO must develop emergency action plans for each facility accommodating a computer system operating in USAID/W for which they are responsible. Such plans must be coordinated with the ISSO for USAID and be consistent with applicable Agency and local government emergency action plans. **(See Additional Help, Contingency Planning for Information Resources)**

d. Mission Emergency Action Plans: The IT Specialist/System Manager and designated site ISSO at a mission must develop site-specific emergency action plans. **(See Additional Help, Contingency Planning for Information Resources)**

e. The IT Specialist/System Manager and designated site ISSO must review, update (if necessary), and test all emergency action plans annually, or when significant modifications are made to system hardware, software, or system personnel.

f. The ISSO for USAID must develop site-specific contingency operation and disaster recovery plans based on threat identification information and system asset accounting and valuation data provided to the ISSO for USAID by the IT Specialist/System Manager and designated site ISSO. **(See Additional Help, Contingency Planning for Information Resources)**

g. Users must protect classified data processed in the stand-alone mode.

h. The Office of Security, in coordination with the Regional Security Officer (RSO) where appropriate, can assist the requesting Bureau, Office, or Mission in determining and installing appropriate physical security controls. **(See ADS 562, Physical Security Programs (Overseas), and ADS 565, Physical Security Programs (Domestic))**

552.3.7 Host Facility System Security Standards

The following policies apply when classified processing is performed at Agency facilities by non-Agency personnel or when Agency personnel must process classified information at other U.S. Government facilities.

a. When Agency facilities, organizations, personnel, or contractors are hosting U.S. cleared personnel not associated with USAID and classified processing on USAID systems is required, the computer security policies and procedures of USAID apply.

b. When cleared U.S. personnel representing the Agency are processing classified information in U.S. Government facilities not operated by USAID, or on non-USAID systems, use the computer security policies and procedures of the host department or agency.

c. If there is a conflict as to which computer security policies and procedures apply, use the computer security policies and procedures of USAID.

552.3.8 Secure Telephone Units (STU-III) or Secure Telephone Equipment (STE), and Their Connection to Fax Equipment

The USAID COMSEC Officer is responsible for facsimile (fax) communications via STU-III or STE involving classified information. All USAID organizations with STU-III or STE must comply with the following security policies.

552.3.8.1 Procurement of STU III/STE

This guidance must be followed when purchasing STU-III or STE and fax equipment in USAID/W.

a. Fax equipment to be connected to a STU-III or STE unit must be procured through the COMSEC Officer for USAID.

b. Fax equipment that must be connected to STU-III or STE devices must not be configured to permit data storage.

c. Only approved STU-III or STE devices will be procured for sensitive or classified data transmissions.

d. STU-III, STE, and secure fax devices must be transported overseas by secure diplomatic pouch. Within the United States, this equipment must be transported by either registered U.S. mail or by U.S. citizens having at least a SECRET clearance.

552.3.8.2 Installation and Repair of STU-III/STE and Secure Fax Equipment

The following requirements must be met when installing or repairing STU-III or STE and fax equipment at USAID facilities:

a. The COMSEC Officer for USAID, in coordination with SEC, must approve the installation of all classified fax devices within USAID/W facilities. You must get SEC approval before installing STU-III, STE, and secure fax equipment.

b. The COMSEC custodian must ensure that the STU-III or STE and attached fax equipment are located in an area approved to accommodate classified information and are configured correctly.

(1) STU-III or STE devices must be connected to classified fax devices by a data port. STU III or STE devices must not be configured to allow auto answer or auto secure.

(2) For STU-III or STE units that allow data transmissions in the clear mode, the COMSEC custodian must use the appropriate cryptographic methodology to configure the STE for encrypted mode processing only.

c. Maintenance of classified fax and STU-III or STE data port connections must be performed by technicians who are U.S. citizens with appropriate level security clearances.

552.3.8.3 Transmissions on STU-III/STE

The following requirements must be followed when transmitting information using STU-III or STE units connected to fax equipment in USAID/W and at missions:

a. Users must not allow data transmission in an unencrypted mode at any time during a STU-III or STE and classified fax connection.

b. Transmissions must be continuously observed during both data transmission and reception. Ask the person sending the secure fax how many pages will be transmitted and make sure all pages have been received/printed before moving away from the secure fax equipment. If the paper supply is low, only a part of the transmission will print. Then someone who later adds more paper could receive classified data not intended for them.

c. Users sending and receiving classified fax transmissions must ensure that terminal display information is correct and that transmissions do not exceed the classification level indicated on the terminal display. For example, if a STU-III or STE unit has only been authorized to transmit/receive CONFIDENTIAL data, do not use that unit to transmit or receive SECRET data.

552.3.8.4 Administrative Management of STU-III/STE

The following administrative requirements must be met whenever secure STU-III or STE equipment is connected to fax equipment in USAID/W and at missions.

a. Labeling Equipment, Posting Requirements

(1) The COMSEC custodian must ensure that fax equipment authorized to transmit classified information is clearly labeled, "EQUIPMENT IS AUTHORIZED FOR TRANSMISSION OF CLASSIFIED INFORMATION UP TO THE CONFIDENTIAL LEVEL,"

or

"EQUIPMENT IS AUTHORIZED FOR TRANSMISSION OF CLASSIFIED INFORMATION UP TO THE SECRET LEVEL."

(2) The COMSEC custodian must ensure that the security requirements or operating classified fax equipment are prominently posted near all functioning classified fax equipment.

b. Personnel Responsibility

(1) The Mission COMSEC Custodian must ensure that all personnel accessing communication devices authorized to transmit sensitive information have the need-to-know in performance of their official duties, appropriate supervision, and knowledge of their communications security responsibilities.

(2) Only the COMSEC custodian will access the master cryptographic materials.

c. Cover Sheets and Logs

(1) Users are responsible for ensuring that each outgoing fax transmission has a cover sheet clearly indicating the classification level, date and time of transmission, subject of the document, number of pages, and the sender's and addressee's name, organization, and fax and office telephone numbers. **(See Additional Help, Sample Fax Cover Sheet)**

(2) The designated site ISSO must ensure that a log of all communications transmitted via a STU-III or STE connection to a fax machine is maintained for at least six months. At a minimum, the communications transmission log must indicate the classification or sensitivity level of the data transmitted, date, time, subject matter, and organizations and personnel sending and receiving fax communications.

552.4 MANDATORY REFERENCES

552.4.1 External Mandatory References

a. Relevant Federal statutes

1. **The Computer Fraud and Abuse Act of 1986, Public Law 99-474, as amended by the National Information Infrastructure Protection Act of 1996, Public Law 104-294**

2. **The Computer Security Act of 1987, Public Law 100-235, as amended by Public Law 104-106, National Defense Authorization Act (Fiscal Year 1996) Division E, Information Technology Management Reform (Clinger-Cohen Act) see also 44 United States Code (U.S.C.) Chapter 35 {Coordination of Federal Information Policy - amended October 30, 2000, by Government Information Security Reform [GISR] Subtitle G of the FY 2001 DoD Authorization Act, Public Law 106-398, as implemented by OMB M-01-08, Guidance On Implementing the Government Information Security Reform Act (January 16, 2000).**

3. **The Electronic Communications Privacy Act of 1986, Public Law 99-508, as amended**

4. **The Freedom of Information Act of 1966, Public Law 89-554, as amended**

5. **The Identity Theft and Assumption Deterrence Act of 1998, Public Law 105-318**

6. **(Section 587 of the Fiscal Year 1999) The Omnibus Appropriations Act, Public Law 105-277, as amended**

7. The Omnibus Diplomatic Security and Anti-terrorism Act of 1986, as amended

8. **The Privacy Act of 1974, Public Law 93-579, as amended**

9. **The Trade Secrets Act of 1948 & 1980, Public Law 96-349, as amended**

b. Executive Orders (EOs)

1. **EO 10450, "Security requirements for Government employment"**

2. **EO 12656, "Assignment of Emergency Preparedness Responsibilities"**

3. **EO 12829, "National Industrial Security Program" (as amended)**

4. **EO 12958, "Classified National Security Information" (as amended)**

5. EO 12968, "Access to Classified Information"

6. EO 13103, "Computer Software Piracy" as Amended

7. EO 13011, "Federal Information Technology"

c. Circulars, Handbooks, Instructions, Manuals, and Regulations

1. 32 CFR Part 154, "Department of Defense Personnel Security Program Regulation"

2. 32 CFR Part 2004, "Safeguarding Classified National Security Information" and associated implementing guidance

3. DOD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria"

***4. DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM)**

5. 12 FAH-6 (OSPB Security Standards and Policy Handbook)

6. 12 FAM 090, Definitions of Diplomatic Security Terms

7. 12 FAM 500, Information Security

8. 12 FAM 600, Information Security Technology

9. National Information Assurance Certification and Accreditation Process (NIACAP, National Security Telecommunications and Information Systems Security Instruction {NSTISSI} No. 1000)

10. OMB Circular A-123, Management Accountability and Control (as revised)

11. OMB Circular A-130, Appendix III, Management of Federal Information Resources

552.4.2 Internal Mandatory References

a. AID Form 500-1 (Request for Issue (Reissue) of Building Pass) [Note: This document is only available on the intranet (http://inside.usaid.gov/forms/). Please contact ads@usaid.gov if you need a copy.]

b. **AID Form 500-3 (Security Investigation and Clearance Record) [Note: This document is only available on the intranet (http://inside.usaid.gov/forms/). Please contact ads@usaid.gov if you need a copy.]**

c. **AID Form 545-2, Authorized Access List**

d. **AID Form 545-6, Visitors Log**

e. **AID Form 552-1, Classified Processing Compliance Review**

f. **AID Form 552-2, USAID Classified Information System User Agreement**

g. **AID Form 6-1 (Request for Security Action) [Note: This document is only available on the intranet (http://inside.usaid.gov/forms/). Please contact ads@usaid.gov if you need a copy.]**

h. **ADS 530, Emergency Planning Overseas**

i. **ADS 531, Continuity of Operations Program**

j. **ADS 545, Information Systems Security**

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

l. **ADS 561, Security Responsibilities**

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

n. **ADS 565, Physical Security Programs (Domestic)**

o. **ADS 566, U.S. Direct-Hire and PASA/RSSA Personnel Security Program**

p. **ADS 567, Classified Contracts, Grants, Cooperative Agreements, and Contractor/Recipient Personnel Security**

q. **ADS 568, National Security Information and Counterintelligence Security Program**

r. **Information Technology Security Roles and Responsibilities**

552.5 ADDITIONAL HELP

a. **Approval to Access and Process Classified National Security Information via Information Systems**

b. **Information System Certification and Approval to Operate**

c. **Contingency Planning for Information Resources**

d. **Sample Fax Cover Sheet**

e. **Selected Security Guidance**

552.6 DEFINITIONS

All ADS chapter terms and definitions are included in the ADS Glossary. Therefore, the terms and definitions listed below have been incorporated into the ADS Glossary. (See **ADS Glossary**)

Classified National Security Information (Classified Information)
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)

encryption
Protecting information by encoding it through use of logarithmic coding keys. (Chapters 545, 552)

Information System (IS)
The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. **This term includes both automated and manual information systems; its acronym is "IS."** (source: NSTISSI 4009) (Chapters 545, 552)

Information Technology Architecture
The term "information technology architecture" means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals. (source: 40 U.S.C. Section 1425) (Chapters 545, 552)

Information Technology
The term "information technology" means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. (source: 40 U.S.C. Section 1401) (Chapters 545, 552)

magnetic media
Devices which can be used to record information in digital form, such as tapes, floppy disks, compact disks (CDs), hard disks etc. (Chapters 545, 552)

Mission Critical System
The term “mission critical system” means any telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that

a. Is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);

b. Is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive Order or an Act of Congress to be classified in the interest of national defense or foreign policy; or

c. Processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of would have a debilitating impact on the mission of an agency. (source: Public Law 106-398) (Chapters 545, 552)

National Security System
The term “national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which

a. Involves intelligence activities;

b. Involves cryptologic activities related to national security;

c. Involves command and control of military forces;

d. Involves equipment that is an integral part of a weapon or weapons system; or

e. Is critical to the direct fulfillment of military or intelligence missions. This final subcategory does not include does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Source: 40 U.S.C.1452) (Chapters 545, 552)

Program Manager
Government official responsible and accountable for the conduct of a Government program. A Government program may be large (e.g., may provide U.S. assistance to other nations); it may also be a support activity such as the Agency's personnel or payroll program. (Chapters 545, 552)

Sensitive Information (also referred to as **Sensitive But Unclassified (SBU)**)
Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of the Agency to accomplish its mission, proprietary data, records requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. It is also certain sensitive official information and material which is not national security information, and therefore, is not classifiable, but nevertheless warrants a degree of protection. Such information or material may include, among other things, information received through privileged sources and certain personnel, medical, investigative, commercial, and financial records. Material of this type which requires protection and limited dissemination shall be designated by any official having signing authority for the material. (Chapters 545, 552, 562, 566, 567)

TEMPEST
The investigation, study, and control of compromising electromagnetic emanations from telecommunications and IS equipment. Sometimes refers to system components that use approved emanation suppression/containment systems for the processing and storage of classified national security information. (Chapters 545, 552, 562)

552_071504_w072304_cd36