ADS Chapter 545

Information Systems Security

Revision Date: 06/12/2006
Responsible Office: M/DCIO
File Name: 545_061206_cd44

Functional Series 500 – Management Services
ADS 545 – Information Systems Security

Table of Contents

Chapter 545 – Information Systems Security

545.1 OVERVIEW

Effective Date – 07/25/2005

Automated Directives System (ADS) Chapter 545 details the security policies, consistent with federal regulations, mandates, and directives, which serve as the highest-level basis for information systems security within USAID. The Office of Management and Budget (OMB) **Circular A-130** requires that USAID provide "adequate security" for its information systems and data—defined as security measures "commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." The **Federal Information Security Management Act of 2002** (FISMA) states each federal agency must implement an agency-wide information security program to protect its operations and assets.

Federal mandates also require that USAID's information systems and applications are operated effectively, and are provided with "appropriate confidentiality, integrity and availability" through the use of cost-effective management, operational, and technical controls.

The security policies specified in this chapter are general statements that set out the mandatory requirements to ensure that a minimum security level is established and maintained for USAID's information systems. These security policies are driven by Public Laws, Executive Orders, other agencies, and existing USAID directives, which are listed as mandatory references. This chapter contains three security policy types. They are specified in the National Institute of Standards and Technology (NIST) **Special Publication (SP) 800-14**, *Generally Accepted Principles and Practices for Securing Information Technology Systems*:

a. Program-specific policies. These define the information security program (infrastructure), set agency-specific strategic direction, assign responsibility within the infrastructure, and address compliance with policy. These policies span USAID.

b. System-specific policies. These apply to single systems, and often address the specific context for meeting the security objectives for that system.

c. Issue-specific policies. These address specific areas of relevance and concern to the Agency (e.g., e-mail, Internet connectivity, mobile device use). These span the entire Agency, and often contain position statements on technology.

NIST **SP 800-12**, *An Introduction to Computer Security: The NIST Handbook* defines three types of security controls: managerial (see 545.3.1), operational (see 545.3.2), and technical (see 545.3.3). This chapter contains information security policies for all three control types. The policy directives in this chapter follow the outline specified for security controls under NIST SP 800-12.

Several documents types support ADS Chapter 545: these include plans, procedures, rules of behavior (ROB), standards, checklists and guidelines. Traceability throughout ADS Chapter 545 and its supporting subdocuments are maintained through the NIST SP 800-12 specified framework. Any security plan, procedure, rule of behavior, standard, checklist, or guideline is traceable to its corresponding security policy in ADS Chapter 545.

In ADS Chapter 545, the term system refers to any USAID information system or application, and may be used to designate both the hardware and software that comprise the information system or application.

The term staff refers to any USAID employee, contractor, or any other individual providing services, either directly or indirectly, to USAID. Staff may or may not be authorized to use USAID information systems. Staff can be individuals who have physical access to a USAID information system without having authorized access to the information system.

The terms user or users refers to any USAID employee or contractor, or other individual, with authorized access to any USAID information systems. The staff classification includes unauthorized individuals who attempt to access USAID information systems. Once the unauthorized individual gains access to a USAID information system, the security policies for users also apply.

The security policies within ADS Chapter 545 apply to unclassified and Sensitive But Unclassified (SBU) systems within USAID. For information on classified information systems processing, see ADS 552, Classified Information Systems Security.

545.2 PRIMARY RESPONSIBILITIES

Effective Date – 07/25/2005

a. The **Chief Information Security Officer (CISO)**, designated by the USAID Chief Information Officer, is directly responsible for overseeing and executing USAID's information systems security program. The CISO is responsible for developing and implementing plans and procedures for:

- Detecting, reporting, and responding to security incidents;
- Notifying the Office of Inspector General (OIG) about security incidents involving any apparent violation of laws, rules, or regulations; and

- Notifying and consulting with other offices and authorities, to include the Department of Homeland Security, and the United States Computer Emergency Readiness Team (US-CERT), in the event that a significant security incident occurs.

b. **USAID staff** are classified into the following categories defined by functionality:

- **Users**. All individuals who are authorized to access and use the USAID network and the systems supported by it, and who have received favorable employment eligibility status or successfully passed a background check or investigation. Users are the only classification that cannot possess elevated privileges.

- **Staff**. This term is included here, but it is not a category into which USAID personnel have been classified. It refers to any USAID employee, contractor, or any other individual providing services, either directly or indirectly, to USAID. Staff may or may not be authorized to use USAID information systems.

- **System Administrators**. A subclass of general users, whose roles within USAID require that they possess elevated privileges for the USAID network or a specific system, and who are able to perform higher-order tasks, including technical operations, which are prohibited for general users.

- **Functional Managers**. A subclass of general users, whose roles and responsibilities within USAID require that they possess elevated privileges for the USAID network or a specific system, and who are responsible for the daily program and operational management of their specific USAID system (including the USAID network).

- **Information System Security Officers (ISSO)**. A subclass of general users, whose roles and responsibilities within USAID require that they possess elevated privileges for the USAID network, a Mission, or a specific system, with privileges sufficient to monitor and enforce the security policies that apply to USAID.

- **Executive Managers**. A subclass of general users, whose roles and responsibilities are specific to the management of USAID and its Missions.

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, defines each of these five roles individually. Specific responsibilities defined for the other four roles (System Administrator, Functional Manager, ISSO, and Executive Manager) may supersede the responsibilities defined for Users. Responsibilities that are designated for the other four roles, that supersede the user responsibilities, may also directly contradict them. For example, users must not test for system vulnerabilities. USAID policy (see 545.3.2.7) designates that this responsibility is restricted to the System Administrator and ISSO roles.

In practice, there will be some "mixing" of the roles. System Managers may have responsibilities from both the System Administrator and Functional Manager roles – the System Administrator role has no management responsibilities. System Managers may also have responsibilities designated to the ISSO role, such as user account management and system vulnerability management.

The roles, as defined, apply across the positions that compose that type. Policies, procedures, rules of behavior, standards, checklists, and guidelines that apply to a role apply to all positions that compose that role. For example, guidance that applies to the ISSO role applies to the Mission ISSOs, System ISSOs, and other personnel whose position descriptions incorporate information system security functions. The guidance that applies to the System Administrator role applies to system administrators, network administrators, firewall administrators, System Managers, Computer Managers, and others whose duties include day-to-day technical operations. The guidance that applies to the Functional Manager role applies to System Owners, System Managers, Computer Managers, and others whose duties include day-to-day management of information systems.

545.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date – 07/25/2005

This section contains USAID's information system security policies, organized by policy type, as specified in 545.1. a, b and c.

This section contains only information security policies. The plans, procedures, rules of behavior, standards, checklists and guidelines derived from these information security policies are detailed in separate documents that are hyperlinked at the end of each subsection, and are listed as mandatory references.

The CISO is empowered by Agency memorandum to alter the policies in Section 545.3 in order to maintain the security of all USAID Sensitive But Unclassified information systems. For classified information systems, refer to ADS 552, Classified Information Systems Security. Changes to USAID's information security policies must go through the ADS clearance process.

The policy and its supporting documents are divided into the following document types:

Policy refers to a document that includes mandatory guidance (policy) as well as broader official statements of Agency goals and objectives.

Plan refers to a document that lays out a specific set of objectives and the means of accomplishing them.

Procedure refers to a document that defines a mandatory course of action or steps that must be followed in order to complete a specific task.

Rule of Behavior refers to a document that contains rules that clearly delineate responsibilities and expected behavior of all individuals with access to a system.

Directive refers to a written instruction communicating policy and/or procedure in the form of orders, regulations, bulletins, circulars, handbooks, manuals, notices, numbered memorandums, and similar issuances.

Standard Under its statutory responsibilities, NIST develops standards and guidelines to protect sensitive federal systems. Some of these standards, formally known as Federal Information Processing Standards have been made mandatory for Federal use by the Secretary of Commerce.

Checklist refers to a list of actions items, steps, or elements needed for a given task.

Guideline refers to an optional or new practice, often based on best practice. Guidelines are not mandatory.

545.3.1 Managerial Policies
Effective Date – 07/25/2005

The following policies state management and top-level functions of the USAID information security program. These policies assign broad staff responsibilities, define the program's basic scope within the organization, and address compliance issues.

Certain policies state that a specific individual, for instance, a System Owner, is responsible for certain activities. The individual assigned the responsibility may not have the technical skills or the appropriate level of knowledge to conduct the activities to meet the policy requirements. In such cases, the named individual must assign staff to perform the required activities. The designated individual may reassign performance of the activity to other individuals, but the responsibility for ensuring that the activities are completed remains with the assigned individual. For example, a System Owner (a functional manager) is required to conduct certification and accreditation activities for their information systems. The level of effort and technical knowledge required to conduct these activities are typically designated to a team of individuals. The System Owner is still responsible for ensuring that the activities are completed.

545.3.1.1 Broad Organizational Policies
Effective Date – 07/25/2005

The following policies apply "broadly" to all USAID information systems across the agency.

a. Staff must adhere to the security policy contained in ADS 545, and the plans, procedures, rules of behavior, standards, checklists, and guidelines derived from them.

b. Staff must use information systems only for USAID business or other limited, Federally authorized use.

c. Staff must only process information on systems that are approved for processing at the same security level or higher than that of the information being processed.

d. Staff must not participate in unethical, illegal or inappropriate activities, such as, but not limited to, pirating software, stealing passwords, stealing credit card numbers, and viewing/exchanging inappropriate written or graphic material (e.g., pornography).

e. Users have no reasonable expectation of privacy when using any USAID information systems. USAID will protect the privacy of specific personally identifiable information as required by law.

f. Staff must safeguard USAID information/data.

g. Staff must not bypass, modify, deactivate or intentionally probe security controls used to protect USAID's information systems without written approval from the CISO.

h. Information System Security Officers, System Administrators and other privileged users must not test, bypass, modify, or deactivate security controls used to protect USAID's information systems, unless authorized in writing to do so by the CISO.

i. The CISO may issue waivers against USAID policy, where permissible by Federal regulation. The supporting documentation for the waiver must contain at least:

- The specific conditions that necessitate the waiver,
- The risk assumed with accepting the conditions,
- The waiver limitations,
- The rationale justifying a decision to waive policy, and
- The time frame that the waiver remains in force.

j. The CISO may monitor any device attached to the network at any time.

k. The General Support System (GSS) ISSO must specify the points of control for Agency computing and telephony resources.

l. The Agency must specify a Record Retention Standard (RRS) for records retained to support information security policy (e.g., audit logs, incident reports, computer forensics that support disciplinary actions, etc.).

545.3.1.2 Penalties and Disciplinary Actions
Effective Date – 07/25/2005

The following policy states the potential consequences that may result from policy infractions committed by staff.

Staff who either intentionally or inadvertently misuse USAID automated resources or do not comply with the policies in ADS 545 or with the plans, procedures and rules of behavior derived from them, may be subject to the full range of administrative disciplinary actions as defined in ADS 485 or ADS 487, as applicable. These sanctions may include

- Counseling, remedial training, revocation of access privileges, and possibly termination.
- Contractor employees can have their access privileges revoked; their contract itself could be partially terminated as a result of an infraction.
- Where such actions appear to be criminal in nature, the matter must be referred to the appropriate Assistant U.S. Attorney by the USAID Inspector General.

545.3.1.3 Program Management
Effective Date – 07/25/2005

The following policies state the information system security program management responsibilities for USAID. Program management, in this context, is the process of creating and managing the USAID information security program, including the policies and enforcement guidelines that are designed to protect USAID's voice/data network equipment, computers and information.

a. The CISO must establish and maintain an information system security program.

b. The CISO must establish and maintain information system security enforcement guidelines to protect USAID information systems.

c. The Agency must explicitly define the information security role in information technology investments and capital programming to comply with Federal regulations.

545.3.1.4 Risk Management
Effective Date – 07/25/2005

The following policies state the risk management responsibilities at USAID. Risk management is the process of identifying risks, assessing the likelihood of their occurrence, and then taking steps to reduce the risk to an acceptable level (mitigation).

a. The CISO must establish and maintain procedures for establishing the security levels for USAID information systems to comply with Federal regulations.

b. The System Owner and System ISSO must establish a security level for each information system using USAID published procedures and guidelines.

c. The System Owner must conduct an initial risk assessment for each information system using USAID published procedures and guidelines.

d. The System Owner must conduct follow-up risk assessments annually, or whenever the system, or its operating environment, significantly changes.

e. The System Owner, System ISSO, and System Administrator must take corrective or remedial action to mitigate vulnerabilities detected during risk assessments.

f. The CISO must verify that the security level has been correctly established for each USAID information system.

g. The CISO must verify that corrective or remedial actions have been taken by the System Owner, System ISSO, and System Administrator.

The USAID procedures and guidelines for establishing a security level are contained in **Security Level Procedures and Guidelines** (Reserved).

USAID guidelines for conducting risk assessments are contained in **Risk Assessment Guidelines**.

545.3.1.5 Rules of Behavior

Effective Date – 07/25/2005

The following policies state the Rules of Behavior (ROB) responsibilities for USAID information systems. The rules of behavior are documented in role- and system-based subdocuments that are used to support Chapter 545. The rules of behavior clearly delineate the responsibilities and behaviors for each role that staff are expected to perform (rules of behavior may overlap as the staff roles overlap). System Owners, the General Support System (GSS) ISSO, and the CISO must establish and disseminate rules of behavior for each of their respective information systems, so that staff are aware of the security rules that pertain to their particular job functions and roles.

a. The CISO must define and, once defined, maintain a set of rules of behavior for the roles for the USAID network.

b. System Owners must define and, once defined, maintain a set of rules of behavior for each information system for which they are responsible.

c. The CISO must verify the content of the System Rules of Behavior defined by each System Owner.

d. Staff must acknowledge, in writing, receipt of the rules of behavior for each system to which they are to be granted access, prior to accessing each system.

The following references contain the Rules of Behavior for each of the five defined user classifications that have been derived from the information security policies in Chapter 545. Additional Rules of Behavior, defined by the System Owners, for each of their respective USAID information systems, must be filed with the Security Plans for each information system.

- **Rules of Behavior for Users**
- **Rules of Behavior for System Administrators**
- **Rules of Behavior for Functional Management**
- **Rules of Behavior for Information System Security Officers**
- **Rules of Behavior for Executive Management**

545.3.1.6 System Development Life Cycle (SDLC) Planning

Effective Date – 07/25/2005

The following policies state the responsibilities for system development life cycle planning defined for USAID staff. System development life cycle planning, in an information security context, is the standard SDLC process with emphasis on conducting security assessments and selecting the proper security controls. Federal requirements mandate that information system security requirements are identified and tracked, prior to system implementation, to ensure that system security is maintained at the level to which the system has been assessed.

a. The CISO must provide, document, and maintain a framework and guidance for system security and data sensitivity assessments consistent with Federal regulations.

b. The System Owner must

- Conduct a system security and data sensitivity assessment for each information system under development.
- Conduct a privacy impact assessment before
  - developing or procuring IT systems;
  - developing projects that collect, maintain, or disseminate information in identifiable form from or about members of the public; or
  - initiating a new electronic collection of information in identifiable form for 10 or more persons, consistent with the **Paperwork Reduction Act** (excluding agencies, instrumentalities or employees of the federal government).

- Select, for each USAID information system, the appropriate managerial, operational, and technical controls, to maintain security at the level to which the information system has was assessed.

- Select the appropriate managerial, operational, and technical controls, to maintain security at the level to which the information system has was assessed.

c. The CISO must validate, for each USAID information system, that the appropriate managerial, operational, and technical controls, have been selected and implemented by the System Owner.

d. The System Owner must identify and track all security requirements within a system-level configuration management system.

The USAID guidelines for conducting security assessments are contained in **Security Self-Assessment Guidelines** (Reserved).

545.3.1.7 Information Assurance
Effective Date – 07/25/2005

The following policies state the information assurance responsibilities defined for USAID staff. Information assurance is a set of processes within which USAID information systems are reviewed, tested and evaluated, and certified and accredited. Information assurance processes are required under Federal regulations to ensure that the risk from operating each information system is minimized and acceptable before the information system is deployed, and is kept at a minimal level while the system is operational.

The ISSO must establish and maintain procedures for conducting certifications and accreditations, annual security reviews, and system testing and evaluations.

a. Certification and Accreditation (C&A)

Certification and accreditation are the processes by which an information system is assessed to determine if it meets the security requirements for the mission's function and the sensitivity level of information handled.

(1) The System Owner must conduct an initial certification and accreditation for each information system, and successfully receive an authority to operate (ATO) or an interim authority to operate (IATO) before deploy the information system to production.

(2) The System Owner must conduct subsequent certifications and accreditations once every three years, or whenever the system, or its operating environment, significantly changes.

b. Annual Security Review

The annual security review is a periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing:

- Must include testing of management, operational, and technical controls of every information system identified in the inventory,
- May include testing relied on in a evaluation, and
- Must be reviewed at least annually, and approved or disapproved as required by the information security program.

(1) System Owners must conduct annual security reviews against each information system's access privileges and operating practices.

(2) The System Owner must conduct annual, periodic testing and evaluation of the security procedures, and security controls to determine their effectiveness.

c. System Testing and Evaluation (ST&E)

System Test and Evaluation is a technique that can be used to identify IT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results).

(1) The System Owner must evaluate annually the information system security controls, to determine whether the controls sufficiently mitigate risk to maintain operational status.

(2) The CISO must perform at least annual system security checks against all USAID systems.

USAID stated procedures for conducting these three information assurance processes are contained in **Information Assurance Procedures**.

545.3.1.8 Privacy Policy

Effective Date – 07/25/2005

The following policies state the responsibilities for personal information that is stored on USAID's information systems. Personal data is any information that can be individually identified – information that can be bound to the identity of a specific individual. Federal regulations require that personal information be protected from loss, disclosure, or any other unauthorized use.

a. Staff must not enter or store information protected under the **Privacy Act of 1974**, and any subsequent legislation, on any information system, except as required to fulfill an approved USAID objective or business function.

b. Staff must not monitor, access, or disclose an individual worker's communications or files without approval consistent with guidance from the USAID Office of the General Counsel, Senior Privacy Official, the CISO or others, as required by Federal regulations. Additionally, staff may not monitor, access or disclose personally identifiable information, unless:

- A legitimate business need exists that cannot be met by other means,
- The involved individual is unavailable and timing is critical,
- There is cause to suspect criminal activity or policy violation, or
- Monitoring is required by law, regulation, or third-party agreement.

545.3.2 Operational Policies

Effective Date – 07/25/2005

The following policies state the information security responsibilities for USAID staff who perform day-to-day operations that support USAID information systems.

545.3.2.1 Personnel

Effective Date – 07/25/2005

The following policies state the information security responsibilities for managing the staff who use, develop, operate, maintain and support USAID information systems. Personnel management involves tasks such as establishing roles and managing user computer accounts. As staff changes, management must ensure that positions are filled and user access to the system is properly handled.

a. General Personnel Policies

(1) For each position, USAID Management must incorporate the security functions required for that role into the position description for that position. Each position must be developed around the security tenets of individual accountability, least privilege, separation of duties, and need to know.

(2) Potential staff must successfully complete a background checks **or** an employment eligibility form before System Administrators grant them access to any USAID system.

b. Staffing

(1) System Owners must maintain a roster of key technical positions and the individuals who fill them for each USAID system. The roster must be included in the System Security Plan for the information system.

(2) System Owners must cross train staff that fill critical roles to provide redundancy for the functions that those positions perform.

c. User Administration

(1) The CISO must establish and maintain generic **Computer Security User Account Management Procedures** (Reserved).

(2) System Owners must establish a user account management system for each information system, which can be used to handle access control changes.

(3) System Owners and System ISSOs must establish security controls and procedures to govern user administration functions for their system(s).

d. Critical Technical and Human Threat Environments

This policy only applies to personnel located in Missions that bear critical technical or human intelligence threat designations. The Office of Security or the CISO can provide details of which Missions bear these designations.

(1) The Regional Security Officer (RSO) must first approve Foreign Service Nationals (FSN) before they can hold an administrative position in a critical threat environment.

Personnel procedures are contained in **Personnel Security Procedures** (Reserved).

User account management procedures are contained in **Computer Security User Account Management Procedures** (Reserved).

545.3.2.2 Business Continuity Planning and Disaster Recovery Planning

Effective Date – 07/25/2005

The following policies state the responsibilities for business continuity planning (BCP) and disaster recovery planning (DRP) for USAID staff.

Business continuity planning ensures that USAID business functions, which are handled by its information systems, remain uninterrupted through time. BCP involves successfully mitigating the risks to systems from natural or man-made events, and building resilient systems that can overcome the identified risks.

Disaster recovery planning ensures that USAID business functions may be resumed and restored after a natural or man-made disaster that has interrupted processing of one or more information systems. DRP involves creating and maintaining a capability for USAID's business functions to be resumed after a disaster, and to later be restored to normal operational state.

a. Business Continuity Planning

(1) The CISO must establish and maintain USAID basic guidelines for business continuity planning.

(2) System Owners must develop business continuity plans for each system.

(3) The CISO must verify the business continuity plans developed by each System Owner.

(4) System Owners must annually test business continuity plans for each system.

b. Disaster Recovery Planning

(1) The CISO must establish and maintain USAID basic guidelines for disaster recovery planning.

(2) System Owners must develop disaster recovery plans for each system.

(3) The CISO must verify the disaster recovery plans developed by each System Owner.

(4) System Owners must annually test disaster recovery plans for each system.

The CISO-established, USAID basic business continuity planning procedures are stated in **Business Continuity Planning Procedures and Guidelines**.

The CISO-established, USAID basic disaster recovery planning procedures are stated in **Disaster Recovery Planning Procedures and Guidelines**.

545.3.2.3 Incident Handling

Effective Date – 07/25/2005

The following policies state the incident handling responsibilities defined for USAID staff. Incident handling is the capability to recognize, react to, and efficiently handle disruptions in business operations that result from security events or unusual system behavior, such as the disclosure of sensitive information, lost passwords, and system crashes. Solid incident handling policies allow for efficient response when security incidents occur.

a. The CISO must establish and maintain USAID security incident handling procedures that comply with Federal regulations and reporting procedures.

b. The CISO, General Support System (GSS) ISSO, and System ISSOs must train staff to recognize and respond to security incidents.

c. Staff must immediately report suspected or known security incidents as directed in the **Incident Identification and Reporting Procedures**.

d. Staff must follow incident handling procedures as directed by USAID personnel responsible for information security.

The USAID basic incident handling procedures, developed by the CISO, to comply with the US-CERT processes, are contained in **Incident Identification and Reporting Procedures**.

545.3.2.4 Awareness and Training

Effective Date – 07/25/2005

The following policies state the responsibilities of USAID personnel for the initial and ongoing awareness, training, and education of USAID's information system users. Awareness, training and educational programs provide knowledge and instruction for operating USAID information systems and protecting USAID data.

a. Awareness

(1) The CISO must establish and maintain an ongoing information security awareness program.

(2) The CISO must evaluate the information security awareness program to determine its effectiveness, and change it if necessary.

(3) If System Owners and System ISSOs have developed system-specific awareness materials for their information system, staff must receive it before they are given access to the information system.

(4) USAID staff and users must participate in the CISO information security awareness program as required by Federal regulations.

b. Training

(1) The CISO must establish and maintain an ongoing information security training program.

(2) The CISO, System ISSO, System Owner or System Administrator must provide remedial training to users who cause a security incident, after the incident occurs.

(3) The CISO must evaluate the security training program to determine its effectiveness, and change it if necessary.

(4) Staff with security responsibilities must maintain their security training by taking information security specific training as required by Federal regulations.

(5) If System Owners and System ISSOs have developed system-specific training for their information system, staff must receive it before they are given access to the information system.

545.3.2.5 User Support

Effective Date – 07/25/2005

The following policies state that USAID must establish a user support capability to generate an initial response and react to a reported security incident.

a. The Agency must establish a user support capability, such as a Help Desk, to support basic user security functions (e.g., password changes, anti-virus support, incident reporting, etc.).

b. The Help Desk, System Administrators, or information security staff must follow incident reporting procedures, developed and documented by the CISO, the GSS Security Operations Staff, and System ISSOs, and must act immediately if a security incident is reported.

c. The Help Desk or System Administrators must document all reported security incidents, as specified in the USAID basic or system-specific incident reporting procedures.

d. System Owners and ISSOs must document information system-specific help desk and incident handling procedures in their information systems' System Security Plans.

545.3.2.6 Software Support

Effective Date – 07/25/2005

The following policies state the responsibilities that are assigned to USAID personnel regarding software support. Software support controls what software operates on information systems, in this context, those specific to USAID, ensuring that the software is free of harmful code, such as viruses, Trojans and worms.

a. General Software Support

(1) The CISO must establish and maintain procedures for evaluating the security risks of new and existing software.

(2) The CISO, in conjunction with the GSS ISSO, must establish a capability for detecting disapproved software changes to, and malicious software operating within, the USAID network.

(3) System Owners and ISSOs must implement security controls on their information systems, or use a capability provided by the CISO or the GSS ISSO, to detect changes to software on each system.

(4) System Managers and Administrators may only attach workstations to the USAID network that are configured with the standard USAID desktop image.

(5) The Information Resources Management (IRM) Change Control Board (CCB) must approve all software that may be installed on any USAID information system.

(6) System Administrators must install only approved software on any USAID information system.

b. Protection against Malicious Software

(1) The CISO must establish and maintain procedures for detection of viruses and other types of malicious software.

(2) The System Administrators and Help Desk must follow the established procedures for detecting viruses, Trojans, and other types of malicious software.

(3) Staff must not alter or disable anti-virus software on any workstation or server.

c. Software Baseline

(1) The IRM CCB must establish and maintain a software baseline of all software approved for use by the USAID.

USAID stated virus detection guidelines are contained in **Virus Detection Guidelines**.

USAID patch management guidelines are contained in **Patch Management Guidelines** (Reserved).

545.3.2.7 Software Development and Maintenance

Effective Date – 07/25/2005

The following policies state the responsibilities for secure software development, documentation, and maintenance by USAID personnel. Secure software development is the creation of software that meets or exceeds the requirements for emplacing security controls at the level to which the system has been assessed. Software documentation includes the controls used to monitor the installation of, and updates to, operating system software, and other software to ensure that the software function as expected, and that a historical record is maintained of application changes. Maintenance is the modifying of software to add, change or deactivate security controls. Secure software development, documentation, and maintenance are necessary to prevent software-based security risks.

a. Software Development

(1) System Owners must maintain a separate development environment for their information systems. USAID production environments, including AIDNET, must not be used for any development activity.

(2) System Owners must ensure that software unnecessary for production server operation is removed from production servers (e.g., compilers, debuggers, and utilities).

(3) System development personnel must not develop software for USAID that incorporates “backdoors,” deactivation mechanisms, and other undocumented functions that could be used to compromise security.

(4) System Owners and ISSOs must document all software features and functions that constitute the information system security controls.

(5) The CISO and the Office for Information Resources Management must establish a capability to evaluate new software for interoperability problems with the existing software baseline.

b. Software Maintenance

(1) The CISO and the Office for Information Resources Management must establish procedures for installation and roll back of fixes, patches, and scripts of security changes to software.

(2) System Administrators must follow established procedures for implementing fixes, patches, and scripts for software.

(3) The CISO must approve hardware and software used to test information system vulnerabilities.

(4) Users must not use hardware or software for testing information system vulnerabilities.

(5) Only ISSOs and System Administrators, with CISO approval, may use hardware or software for testing information system vulnerabilities.

545.3.2.8 Configuration Management

Effective Date – 07/25/2005

The following policies state the responsibilities for configuration management by USAID personnel. Configuration Management is the process by which the configuration of an item and its components are identified and documented, and changes are controlled and tracked. The goal of the configuration management process makes it easier to detect any changes to hardware or software within an information system.

a. System Owners must develop and use configuration management procedures for all production information systems.

b. The CISO and Office for Information Resources Management must implement formal procedures to evaluate all revised hardware and/or software prior to implementation.

c. System Owners must maintain an accurate inventory of system software, hardware and configurations.

545.3.2.9 Physical Facilities and Restricted Spaces

Effective Date – 07/25/2005

The following policies state the responsibilities of USAID personnel to protect its physical environments and to maintain security by emplacing physical security controls. Factors to be considered when assessing physical facilities and restricted spaces include:

- Environmental controls,
- Natural physical risks (such as storms, floods, and other naturally occurring events),
- Man-made physical risks (such as unauthorized physical access, terrorist activities), and
- Environmental risks such as heating, cooling, and power loss.

a. Physical Facilities

(1) The CISO must establish and maintain guidelines for conducting annual physical review of facilities that house USAID information systems.

(2) One or more of; Office of Security (SEC), the CISO, the GSS ISSO, or the System ISSO must approve facilities that are located in the continental United States and that contain USAID information systems or house USAID staff.

(3) The Department of State must approve facilities that are located outside the continental United States that contain USAID information systems or house USAID staff.

(4) The CISO must conduct an annual physical review of contractor-managed facilities within the continental United States.

(5) The Office of Security must conduct an annual physical review of government-managed facilities within the continental United States.

b. Restricted Space (Server Rooms, Telecommunications Closets, etc.)

(1) Staff and visitors must follow restricted access procedures, including signing in and properly escorting visitors.

(2) Only staff on the authorized access list for a restricted space may escort individuals within that restricted spaces.

(3) Staff and visitors who are not on the authorized access list for a restricted space must sign a visitors log (prior to admission), and be escorted and monitored by staff on the authorized access list while in the restricted space.

Physical facilities and restricted spaces security procedures are contained in **Restricted Access Procedures and Guidelines**.

545.3.2.10 Networks and Workstation Connectivity

Effective Date – 07/25/2005

The following policies govern network and workstation connectivity, i.e., the interlinking of computers across one or more physical sites. Management must take steps to keep the network and its devices secure from outside intruders.

a. Networks

(1) The CISO must establish, maintain, and approve procedures for users to access USAID networks.

2) Users must follow established network access procedures.

3) Users must be identified and authenticated prior to accessing the network.

4) Network ports must not be activated in public areas, unless CISO-approved.

(5) System Administrators must configure access controls to network devices to limit or restrict traffic to and from the USAID network.

(6) The CISO must approve and authorize the use of network monitoring and testing equipment.

(7) Users must not use network monitoring and testing equipment.

(8) ISSOs, System Administrators, and other privileged users must not use network monitoring and testing equipment, unless authorized to do so by the CISO.

(9) Staff must not publicly release any information about USAID networks without the approval of the CISO, the GSS ISSO, or their System ISSO.

(10) Users must not alter the USAID network by changing settings for network devices or by adding or removing equipment to the USAID network.

(11) Users must not use modems, 802.11, Bluetooth or other wireless devices unless CISO-approved.

(12) System Administrators must deploy and use USAID-approved time servers.

(13) System Administrators must not further implement or expand their use of Dynamic Host Configuration Protocol on any USAID network without the express permission of the IRM CCB.

b. Firewalls

(1) The CISO must establish and maintain firewall standards, configuration management and operating procedures.

(2) System Administrators must follow established firewall standards and procedures.

(3) System Administrators must regulate all traffic traveling between lesser trusted networks, to include the Internet, and the USAID network, by passing it through a firewall.

(4) The GSS ISSO must approve the use of firewalls and all changes to them, using CISO approved procedures.

(5) System Administrators must validate new firewall configurations, and the new configuration must be approved by the GSS ISSO and the IRM CCB before production deployment.

(6) System Administrators must run firewalls on dedicated machines.

(7) System Administrators and the GSS ISSO must evaluate and approve all new firewalls and new connectivity paths for security risks.

(8) System Administrators must log all changes to firewalls.

(9) System Administrators and the GSS ISSO must periodically review firewall logs to check for anomalies.

(10) System Administrators must maintain and respond to current information about firewall vulnerabilities. Firewall vulnerability information may be obtained from user groups, manufacturer's web pages, etc.

(11) System Administrators must conduct, on a quarterly basis, or as prescribed by the CISO, a firewall "check" to make sure that old rules are disabled or removed and that the firewall policy has been reviewed.

Firewall Guidelines are contained in **Firewall Guidelines** (Reserved).

c. Production & Development Servers

(1) The CISO, in conjunction with the Office for Information Resources Management, must establish and maintain internal standards for configuration management and procedures for server configuration.

(2) System Administrators must configure servers to conform to internal server security standards.

(3) System Administrators must place Internet-accessible servers in a De-Militarized Zone (DMZ), e.g., web, e-mail, etc.

(4) The System ISSO must approve all significant changes to production servers.

(5) System Administrators and the System ISSO must evaluate all new servers and their interconnections for security risks.

545.3.2.11 Media Controls
Effective Date – 07/25/2005

The following policies state USAID's position on media use and transportation. Media are information storage devices such as tapes, memory sticks, and diskettes, which provide a convenient way to physically move information between systems. Being portable, media must be kept physically secure to prevent theft, loss, or damage.

a. Media Usage

(1) The CISO must establish procedures for securely handling media (i.e., internal and external labeling, transport).

(2) Staff must follow established procedures for media usage and handling.

(3) The CISO must establish data remanence procedures (i.e., disposal and destruction).

(4) Staff must follow CISO-approved data remanence procedures.

(5) Staff must securely store all removable media when not in use.

b. Transporting Media

(1) The CISO must establish guidelines consistent with Federal regulations for securely transporting media to maintain agency control during transport.

(2) Staff must follow established guidelines when transporting media.

Media handling procedures are contained in **Media Handling Procedures and Guidelines**.

Data remanence procedures are contained in **Data Remanence Procedures**.

545.3.2.12 System Maintenance
Effective Date – 07/25/2005

The following policies state USAIDs position on the maintenance of USAID information systems. System maintenance involves the repair and upkeep of systems or devices. Keeping systems and devices running may also require access to system or information by outside personnel. Management must take steps to ensure that maintenance activities are conducted in a manner that maintains security.

a. System Administrators must remove default accounts, where possible. If not possible, System Administrators must deactivate default accounts. Such accounts are typically used for system maintenance.

b. System Administrators must configure or restrict (e.g., strong authentication, remote callback, etc.) access to remote diagnostics so that they can only be used to provide support services, and are disabled when not in use.

c. System Administrators must follow established data remanence procedures for data storage devices submitted for off-site maintenance.

d. System Administrators must restrict those who perform maintenance and repair activities on USAID systems to maintenance personnel who are: 1) either direct-hire federal employees or 2) who are working under a contractual arrangement that includes the appropriate security provisions in accordance with this Chapter or **ADS 552, Classified Information Systems Security**.

545.3.2.13 Backups

Effective Date – 07/25/2005

The following policies state USAID's position on server and workstation backup management, handling, and creation. Backups are the process in which a duplicate copy of software, files, information/data is made on a second medium (a disk or tape) as a precaution in case the original is lost or corrupted. Backups are an important step to preventing information/data loss.

a. The CISO must establish basic USAID standards for conducting information system backups.

b. System Owners must create backup plans for each information system.

c. System Administrators must implement and validate the backup plans for their information systems.

d. Staff must comply with backup procedures for information, contained on their workstations.

545.3.2.14 Information Sharing

Effective Date – 07/25/2005

The following policies state USAID's position on the disclosure of USAID information to other parties. Management must take steps to provide protection for USAID-owned information. These policies provide directives that show how to release, if necessary, internal information to third parties.

a. The CISO must establish guidelines detailing when to disclose, how to disclose, and how to resolve problems with disclosure of USAID information.

b. Staff must follow established disclosure guidelines when releasing information.

Related information may be found in the following documents:

- **ADS 507 - Freedom of Information Act (FOIA),**
- **ADS 508 - Privacy Act - 1974,**
- **ADS 509 - Creating, Altering, or Terminating a System of Records,**
- **ADS 557 - Public Information,**
- **ADS 558 - Public Activity,**
- **ADS 559 - Inquiries from the News Media,** and
- **ADS 560 - News Releases and Services.**

545.3.2.15 Intellectual Property Management

Effective Date – 07/25/2005

The following policies state USAID's position on the handling of intellectual property. Intellectual property is intangible property, such as patents, trademarks and copyrighted materials, that is the result of intellectual effort and is legally protected. Management must ensure the proper handling of such information.

a. All information processed, generated, or stored on any USAID information system is the property of USAID.

b. Staff who work with USAID specific intellectual property, while using any USAID information system, must sign a non-disclosure agreement (NDA).

c. Staff who work with third-party intellectual property while employed by USAID, using any USAID information system, must sign an NDA with the third party when requested to do so.

d. Whenever staff use, store, or distribute copyrighted materials within a USAID information system, they must cite them. Where possible, staff must obtain the permission of the author/owner to use the material.

545.3.3 Technical Policies

Effective Date – 07/25/2005

The following policies state USAID's position on information security topics that involve technical aspects of USAID's information system. These topics address areas such as user identification technology and controlling access to USAID's information system.

545.3.3.1 Identification and Authentication (Passwords)

Effective Date – 07/25/2005

The following policies govern the management of user identification and authentication controls, i.e., passwords. These controls provide access to the network, system, e-mail, and must be carefully managed and administered.

a. The CISO must establish and maintain internal standards for creating and using passwords that are consistent with Federal regulations.

b. System Administrators must configure security controls so that users are identified and authenticated, using UIDs and passwords, or similar authentication mechanism, prior to being granted access to any USAID information system.

c. System Owners and System ISSOs must establish security controls and handling procedures for passwords specific to their system. System Administrators must implement these security controls.

d. A CISO waiver must be obtained whenever a password cannot meet the established password standards.

e. Users must not write down passwords unless they are stored in a CISO-approved secure container.

f. Users must not share their passwords.

g. Users must follow the password standards and procedures.

Password creation standards are contained in **Password Creation Standards and Technical Controls** (Reserved).

545.3.3.2 Logical Access Controls

Effective Date – 07/25/2005

The following policies state the information system access controls. Logical access controls limit or control the types of access the user may have to the system and its contents. Management must ensure that the type and amount of access granted is given only to authorized personnel and is appropriate for the system being accessed.

a. The CISO must establish standards for logical access controls.

545.3.4 System-Specific Policies
Effective Date – 07/25/2005

System-specific policies state information security topics that apply to USAID's information systems, and often addresses the specific context for meeting the security objectives for that system. System-specific policies are determined based upon analysis of USAID-reported major applications and general support systems. System-specific policy must be cleared through the CISO's office.

545.3.5 Issue-Specific Policies
Effective Date – 07/25/2005

The following policies state information security topics for specific areas of relevance and concern to the Agency, within USAID's information system, such as e-mail, Internet connectivity and mobile device use. These span the entire Agency and often contain position statements on technology.

545.3.5.1 Audit Trails and Logs
Effective Date – 07/25/2005

The following policies state the use of audit trails and logs. Audit trails and logs provide a record of user activity on the system. The use of audit trails and logs can help to reduce the likelihood of security incidents.

a. The CISO must establish minimum standards for audit logging.

b. System Owners must establish rules for audit logging, which the CISO must review and approve.

c. System Owners must forward data captured in audit logs to the CISO as requested.

545.3.5.2 Authentication Tokens
Effective Date – 07/25/2005

The following policies state USAID's position on the management of user identification and authentication controls by means of tokens. Authentication tokens are devices given to users who keep them in their possession. To log onto the network, the device may be read directly like a credit card, or it may display a changing number that is typed in as a password. These controls provide access to the network, systems, and e-mail, and must be carefully managed and administered.

a. The CISO must approve all token-based authentication methods.

b. When token-based authentication methods are used, a token management lifecycle must be established and implemented.

c. Staff must be trained in the proper handling of tokens.

545.3.5.3 Biometrics

Effective Date – 07/25/2005

The following policies state USAID's position on the management of user identification and authentication controls by means of biometric devices. Biometric devices use behavioral or physiological characteristics (such as retina scan, iris scan, or fingerprints) to determine or verify a user's identity. These controls provide access to the network, systems, e-mail, and other areas, and must be carefully managed and administered.

a. The CISO must approve all biometric authentication methods.

b. When biometric authentication methods are used, authentication procedures must be developed and implemented.

c. Staff must be trained in the secure usage of biometric devices.

545.3.5.4 Collaboration Software

Effective Date – 07/25/2005

The following policies state USAID's position on the installation and use of collaboration software that provides the ability to connect users at two or more workstations for concurrent work on a specific project. Collaboration software functions commonly includes file sharing, white-boarding, video- or audio-communication, version control, and document management.

a. Staff must not install collaboration software unless approved by the IRM CCB and CISO.

b. Staff must not use collaboration software unless approved by the IRM CCB and the CISO.

c. Staff must disable any remote control capability in collaboration software not approved by the CISO.

545.3.5.5 Cryptography

Effective Date – 07/25/2005

The following policies state USAID's position on the use of encryption. Encryption is the act of transforming information into an unintelligible form, specifically to obscure its meaning or content. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it was not intended, including those who can see the encrypted data. Solid encryption technology is necessary to protect USAID's information.

a. The CISO must establish standards and guidelines for encryption technology.

b. Staff must follow CISO-established standards and guidelines when selecting an encryption technology for a USAID information system.

545.3.5.6 E-Mail

Effective Date – 07/25/2005

The following policies state USAID's position on the usage of electronic communications known as e-mail. E-mail allows communication both between USAID staff, and between USAID staff and outside parties. Improper use of e-mail can cause disruptions, information loss, or otherwise diminish or prevent normal workflow. Management must take steps to ensure that USAID staff use e-mail properly.

a. The Agency must establish an e-mail acceptable use policy.

b. Staff must follow the standards and procedures outlined in the acceptable e-mail use document.

The E-mail acceptable use policy is contained in **E-Mail Acceptable Usage Policy**.

Additional information may be found in **ADS 541, Information Management**.

545.3.5.7 File Sharing Software

Effective Date – 07/25/2005

These policies state USAID's position on the use of file sharing software. File sharing software poses threats to USAID information that include accidental or deliberate release, and malicious corruption, alteration, or deletion.

a. Staff must not install file sharing software unless approved by the IRM CCB and the CISO.

b. Staff must not use file sharing software unless approved by the IRM CCB and the CISO.

545.3.5.8 Freeware

Effective Date – 07/25/2005

The following policies state USAID's position on the use of freeware at USAID. Freeware is software that you can use without cost. Unlike shareware, for which you are required to pay a registration fee, freeware is largely uncontrolled and proprietary (not subject to source review). This may allow malicious code to be included within the software.

a. Staff must not install freeware on any USAID information system unless approved by the IRM CCB and the CISO.

545.3.5.9 Instant Messaging (IM)
Effective Date – 07/25/2005

The following policies state USAID's position on the use of instant messaging. Instant messaging is a service that provides "instant" or real-time communications between people. IM allows them to communicate by sending text messages, sharing files and pictures, and sometimes voice and video.

a. Staff must not install instant messaging software unless approved by the IRM CCB and the CISO.

b. Staff must not use instant messaging software unless approved by the IRM CCB and the CISO.

c. Staff must disable instant messaging software remote control from other workstations.

d. Staff must not use any software or web browsers, for instant messaging.

545.3.5.10 Internet and Intranet Usage
Effective Date – 07/25/2005

The following policies state USAID's position on the use of the Internet. The Internet connects computers from around the world, and includes a vast number of sites. The intranet is internal to USAID and accessible only by USAID and Department of State staff. Management must take steps to ensure that USAID staff use the Internet and intranet properly.

a. The Agency must establish an acceptable use policy for the Internet.

b. The Agency must establish an acceptable use policy for the intranet.

c. Staff must follow the guidelines outlined in the acceptable use policy for the Internet and intranet.

The Internet acceptable use policy is contained in the **Internet Acceptable Usage Policy**.

Additional information may be found in **ADS 541, Information Management**.

545.3.5.11 Internet Radio
Effective Date – 07/25/2005

The following policies state USAID's position on Internet radio reception.

a. Staff must not install Internet radio software unless approved by the IRM CCB and the CISO.

b. Staff must not use Internet radio software unless approved by the IRM CCB and the CISO.

c. Staff must not use software or the web browsers, to listen to Internet radio broadcasts.

545.3.5.12 Mobile Computing Devices

Effective Date – 07/25/2005

The following policies state USAID's position on mobile computing devices for USAID's information system. Mobile computing devices are transportable information processing devices such as laptop computers and Personal Digital Assistants (PDA). These devices are particularly at risk due to their portability and monetary value, and must be properly protected to guard against potential security incidents.

a. The CISO must establish standards for mobile computing devices.

b. The IRM CCB must establish procedures for mobile computing devices.

c. Staff must follow the standards and procedures for mobile computing devices.

d. Staff must not connect non-USAID-issued computing device(s) to the USAID network or information systems.

e. Users should not connect USAID-issued computing device(s) to non-USAID networks or Internet service providers (ISPs), if the devices cannot be configured with anti-virus and firewall software. When connected to non-USAID networks, the anti-virus and firewall software should be operational.

f. System Administrators must examine any USAID-issued computing device, before it is directly connected to the USAID network. If the mobile computing device is found to be insecurely configured or compromised, System Administrators may extract the data from the device and must rebuilt it before connectivity to the USAID network is permitted.

Mobile computing standards and guidelines are contained in **Mobile Computing Standards and Guidelines**.

545.3.5.13 Open Source

Effective Date – 07/25/2005

The following policies state USAID's position on the use of open source software at USAID. For software classified as "open source," the source code is available for viewing, extension, modification, and perhaps free redistribution. Unlike freeware, open

source software is non-proprietary – there exists the potential for peer review. Like freeware, there is often no cost for open source software.

a. Staff must not install open source software unless approved by the IRM CCB and the CISO.

b. If the IRM CCB or CISO have approved, but limited the use of, any open source software, staff must not use it until the IRM CCB and/or the CISO authorize its use.

545.3.5.14 Peer-to-Peer Software

Effective Date – 07/25/2005

The following policies state USAID's position on the use of peer-to-peer (P2P) software. Peer-to-peer software creates a network between computers, in which each computer is both a client and a server. P2P users exchange information between computers using proprietary protocols.

a. Staff must not install peer-to peer software unless approved by the IRM CCB and the CISO.

b. Staff must not use peer-to peer software unless approved by IRM CCB and the CISO.

545.3.5.15 Remote Control Software

Effective Date – 07/25/2005

The following policies state USAID's position on remote control software. Remote control software provides the ability for users to control another computer across a network or to have their computer controlled remotely from across a network. Remote control software may be bundled with other software, such as collaboration software, file sharing software, P2P software, etc.

a. Staff must not install remote control software unless approved by the IRM CCB and the CISO.

b. Staff must not use remote control software unless approved by the IRM CCB and the CISO.

545.3.5.16 Shareware

Effective Date – 07/25/2005

The following policies state USAID's position on the use of shareware. Shareware is software for which you must eventually pay a registration fee. Like freeware, shareware retains its proprietary component (the fee for use), and may or may not include distribution of the source code, like open source software. Like freeware, malicious code may be included in shareware.

a. Staff must not install shareware unless approved by the IRM CCB and the CISO.

b. Staff must not use shareware unless approved by the IRM CCB and the CISO.

545.3.5.17 Spyware and Adware

Effective Date – 07/25/2005

The following policies state USAID's position on the use of spyware and adware detection and prevention software. Spyware and adware collect, without the user's knowledge, information about the user, and relay that information to another individual or company. The information is often used to produce an advertising profile, collected from your Internet surfing habits and personal information stored on your workstation or laptop.

a. Agency-issued laptops must have IRM CCB and CISO-approved spyware and adware detection and removal software installed and properly configured.

b. Staff must not alter or disable spyware or adware detection software on any workstation or laptop.

545.3.5.18 System Hardware and Software Procurement

Effective Date – 07/25/2005

The following policies state USAID's position on system hardware and software procurement for USAID information systems. It is important that hardware and software for USAID be carefully selected in order to mitigate risk.

a. The CISO must establish standards for system hardware and software procurement.

b. System Owners must select hardware and software security components for each system under development from ISSO-approved technologies.

545.3.5.19 Virtual Private Network (VPN)

Effective Date – 07/25/2005

The following policies state USAID's position on the use of virtual private networks. A Virtual Private Network is the concept of using the Internet, or other public carrier, as a transit for private and encrypted network traffic.

a. The CISO must establish VPN standards for USAID.

b. System Owners, when incorporating VPN technology into USAID information systems, must select from CISO-approved technologies.

c. Staff using VPN technology to connect to USAID systems must follow the CISO-established standards.

545.3.5.20 Wireless Access
Effective Date – 07/25/2005

The following policies state USAID's position on wireless network access. Wireless communication provides access to the network without a physical connection. The addition of a wireless device makes it difficult to physically secure access to a network. It is important that wireless access and devices are carefully managed and administered in order to mitigate the risks inherent to wireless technology.

a. The CISO must establish standards for wireless devices.

b. The CISO must approve any use of wireless devices.

c. System Administrator must only install CISO-approved wireless devices.

d. Security staff must maintain a current record of all wireless devices.

e. Users must be identified and authenticated prior to accessing the network via wireless connection.

f. Users must comply with established network policies once a wireless connection has been established.

The wireless access standards are contained in **Wireless Access Standards and Guidelines**.

545.3.5.21 Internet Protocol Version 6 (IPv6)
Effective Date – 07/25/2005

The following policies state USAID's position on the transition, implementation and use of IPv6. This version of internet protocol provides improved address space, quality of service and data security over the current IPv4.

a. The CISO must establish standards and guidelines for IPv6.

b. Staff must follow CISO-established standards and guidelines for IPv6.

545.3.5.22 Critical Threat Postings
Effective Date – 07/25/2005

This section contains policies for environments considered by the agency to be critical threat posts. These threats can be social, political or natural (such as volcano, earthquake or other natural event.).

a. The mission Executive Officer (EXO) must request, the Regional Security Officer (RSO) perform the highest level background investigation available within the host country on Foreign Service Nationals (FSN) prior to employment.

b. Foreign Service Nationals (FSN) may hold administrative positions in critical threat environments.

545.4 MANDATORY REFERENCES

Effective Date: 07/25/2005

This section contains references that shape the agency's security stance and policy.

545.4.1 External Mandatory References

Effective Date: 07/25/2005

545.4.1.1 Federal Statutes

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

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

c. Public Law 96-349, The Trade Secrets Act of 1948 and 1980, as amended.

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

e. Public Law 99-399, The Omnibus Diplomatic Security and Anti-terrorism Act of 1986, as amended.

f. Public Law 103-62, **Government Performance Results Act of 1993**, August 3, 1993.

g. Public Law 103-355, **Federal Acquisition Streamlining Act (FARA) of 1994**, October 13, 1994.

h. Public Law 104-13, **Paperwork Reduction Act of 1995**, May 22, 1995.

i. Public Law 104-104, **Telecommunications Act of 1996**, February 8, 1996.

j. Public Law 104-106, **Division E, The Information Technology Management Reform Act (Clinger-Cohen Act) of 1996.** (Authority)

k. Public Law 104-294, **Title II, National Information Infrastructure Protection Act of 1996**, January 3, 1996.

l. Public Law 105-277, **The Government Paperwork Elimination Act (GPEA)**, as amended.

m. Public Law 105-318, **The Identity Theft and Assumption Deterrence Act of 1988**, as amended.

n. Public Law 106-229, **Electronic Signatures in Global and National Commerce Act (E-Sign) (Public Law 106-229)**, June 30, 2000.

o. Public Law 107-296, **Homeland Security Act of 2002**, November 25, 2002.

p. Public Law 106-398, **Title X, Subtitle G, the Government Information Security Reform Act (GISRA)**.

q. Public Law 107-198, **Small Business Paperwork Relief Act of 2002**, June 28, 2002.

r. Public Law 107-347, **Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002)**, December 2002, as amended. (Authority)

545.4.1.2 Executive Orders (EOs)

a. Executive Order 10450, **Security Requirements for Government Employment, as amended**.

b. Executive Order 12656, **Assignment of Emergency Preparedness Responsibilities**.

c. Executive Order 12845, **Requiring Agencies to Purchase Energy Efficient Computer Equipment**, April 21, 1993.

d. Executive Order 12829, **National Industrial Security Program**, as amended.

e. Executive Order 12958, **Classified National Security Information**, as amended.

f. Executive Order 12968, **Access to Classified Information**.

g. Executive Order 13010, **Critical Infrastructure Protection**, July 16, 1996.

h. Executive Order 13011, **Federal Information Technology**, July 16, 1996. (Authority)

i. Executive Order 13103, **Computer Software Piracy**

j. Executive Order 13111, **Using Technology to Improve Training Opportunities for Federal Government Employees**, January 12, 1999.

k. Executive Order 13130, **National Infrastructure Assurance Council**, July 14, 1999.

l. Executive Order 13166, **Improving Access to Services for Persons with Limited English Proficiency**, August 16, 2000.

m. Executive Order 13228, **Establishing the Office of Homeland Security and the Homeland Security Council**, October 8, 2001. Section 3 (g) and Section 7 of E.O. 13228 are amended by Section 8 (a) and (b) of E.O. 13286 of February 28, 2003.

n. Executive Order 13231, **Critical Infrastructure Protection in the Information Age**, October 16, 2001. Executive Order 13231 was amended in its entirety by Section 7 of Executive Order 13286 of February 28, 2003.

o. Executive Order 13260, **Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security**, March 19, 2002.

p. Executive Order 13283, **Establishing the Office of Global Communications**, January 21, 2003.

q. Executive Order 13284, **Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Establishment of the Department of Homeland Security,** January 23, 2003.

r. Executive Order 13286, **Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security**, February 28, 2003.

s. **The National Strategy To Secure Cyberspace**, February 2003

t. **The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets**, February 2003.

u. Executive Order 13311, **Homeland Security Information Sharing**, July 29, 2003.

545.4.1.3 Memoranda

a. **GSA Memo providing the Recommended Executive Branch Model on "Limited Personal Use" of Government Office Equipment including Information Technology** Approved –May 19, 1999

545.4.1.4 National Security Telecommunications and Information Systems Security Instruction (NSTISSI)

a. NSTISSI 1000, **National Information Assurance Certification and Accreditation Process (NIACAP),** April 2000

b. NSTISSI 4009, **National Information Systems Security (INFOSEC) Glossary**, January 1999.

545.4.1.5 National Archives and Records Administration (NARA)

a. **National Archives and Records Administration (NARA) Records Management Guidance for Agencies Implementing Electronic Signature Technologies**, October 18, 2000.

545.4.1.6 Homeland Security Presidential Directive (HSPD)

a. Homeland Security Presidential Directive HSPD-7, **Critical Infrastructure Identification, Prioritization, and Protection**, December 17, 2003.

b. Homeland Security Presidential Directive HSPD-8, **National Preparedness**, December 17, 2003.

c. Homeland Security Presidential Directive HSPD-11, **Comprehensive Terrorist-Related Screening Procedures**, August 27, 2004.

d. Homeland Security Presidential Directive HSPD-12, **Policy for a Common Identification Standard for Federal Employees and Contractors**, August 27, 2004. (Authority)

545.4.1.7 NIST Special Publications

a. NIST SP 800-4, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, March 1992. *As of October 2003, **800-4 has been superseded by 800-64 Security Considerations in the Information System Development Life Cycle***

b. NIST SP 800-6, **Automated Tools for Testing Computer System Vulnerability**, December 1992. *NIST Archived.*

c. NIST SP 800-12, **An Introduction to Computer Security: The NIST Handbook**, October 1995. (Authority)

d. NIST SP 800-13, **Telecommunications Security Guidelines for Telecommunications Management Network**, October 1995.

e. NIST SP 800-14, **Generally Accepted Principles and Practices for Securing Information Technology Systems**, September 1996. (Authority)

f. NIST SP 800-15, **Minimum Interoperability Specification for PKI Components (MISPC)**, Version 1, September 1997.

g. NIST SP 800-16, Information Technology Security Requirements; A Role- and Performance Based Model, **Part1 Document** , **Part 2 Appendix A-D** , **Part 3 Appendix E**, April 1998. (Authority)

h. NIST SP 800-18, **Guide for Developing Security Plans for Information Technology Systems**, December 1998. (Authority)

i. NIST SP 800-19, **Mobile Agent Security**, October 1999.

j. NIST SP 800-20, **Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS)**: Requirements and Procedures, October 1999. Revised April 2000.

k. *NIST SP 800-21-1, **Second Edition, Guideline for Implementing Cryptography in the Federal Government**, December 2005.

l. NIST SP 800-22, **A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications**, October 2000.

m. NIST SP 800-23, **Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products**, August 2000.

n. NIST SP 800-26, **Security Self-Assessment Guide for Information Technology Systems**, November 2001.

o. NIST SP 800-27, **Engineering Principles for Information Technology Security (A Baseline for Achieving Security)**, June 2004. (Authority)

p. NIST SP 800-28, **Guidelines on Active Content and Mobile Code**, October 2001.

q. NIST SP 800-29, **A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2**, June 2001.

r. NIST SP 800-30, **Risk Management Guide for Information Technology Systems**, July 2002.

s. NIST SP 800-31, **Intrusion Detection Systems**, November 2001.

t. NIST SP 800-33, **Underlying Technical Models for Information Technology Security,** December 2001. (Authority)

u. NIST SP 800-34, **Contingency Planning Guide for Information Technology Systems**, June 2004.

v. NIST SP 800-35, **Guide to Information Technology Security Services**, October 2003.

w. NIST SP 800-36, **Guide to Selecting Information Security Products**, October 2003.

x. *NIST SP 800-37, **Guide for the Security Certification and Accreditation of Federal Information Systems**, May 2004. (Authority)

y. NIST SP 800-40, **Procedures for Handling Security Patches**, September 2002.

z. NIST SP 800-41, **Guidelines on Firewalls and Firewall Policy**, January 2002.

aa. NIST SP 800-42, **Guideline on Network Security Testing**, October 2003.

bb. NIST SP 800-43, **Systems Administration Guidance for Windows 2000 Professional**, November 2002.

cc. NIST SP 800-44, **Guidelines on Securing Public web Servers**, September 2002.

dd. NIST SP 800-45, **Guidelines on Electronic Mail Security**, September 2002.

ee. NIST SP 800-46, **Security for Telecommuting and Broadband Communications**, September 2002.

ff. NIST SP 800-47, **Security Guidelines for Interconnecting Information Technology Systems**, September 2002.

gg. NIST SP 800-48, **Wireless Network Security: 802.11, Bluetooth, and Handheld Devices**, November 2002.

hh. NIST SP 800-49, **Federal S/MIME V3 Client Profile**, November 2002.

ii. NIST SP 800-50, **Building an Information Technology Security Awareness and Training Program**, October 2003.

jj. NIST SP 800-53, **Recommended Security Controls for Federal Information Systems.**

kk. NIST SP 800-55, **Security Metrics Guide for Information Technology Systems**, July 2003.

ll. NIST SP 800-56, **Recommendation on Key Establishment Schemes DRAFT**.

mm. NIST SP 800-57, **Recommendation on Key Management DRAFT**.

nn. NIST SP 800-58, **Security Considerations for Voice Over IP Systems**, January 2005.

oo. NIST SP 800-59, **Guideline for Identifying an Information System as a National Security System**, August 2003.

pp. NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, **Volume I**, **Volume II - Appendix**, June 2004. (Authority)

qq. NIST SP 800-61, **Computer Security Incident Handling Guide**, January 2004.

rr. NIST SP 800-63, **Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology**, June 2004. Revision 1.0.1 released September 2004.

ss. NIST SP 800-64, **Security Considerations in the Information System Development Life Cycle**, October 2003. (Authority)

tt. NIST SP 800-65, **Integrating Security into the Capital Planning and Investment Control Process**, January 2005.

uu. NIST SP 800-66, **An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule**, March 2005.

vv. NIST SP 800-67, **Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher**, May 2004.

ww. NIST SP 800-68, **Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist DRAFT**.

xx. NIST SP 800-70, **The NIST Security Configuration Checklists Program** , May 26, 2005.

yy. NIST SP 800-72, **Guidelines on PDA Forensics**, November 2004.

zz. *NIST SP 800-73, Revision 1, **Integrated Circuit Card for Personal Identity Verification**, April 12, 2005.

545.4.1.8 NIST Federal Information Processing Standards

a. FIPS PUB 101, Guideline for Life Cycle Validation, Verification, and Testing of Computer Software, June 6, 1983.

b. FIPS PUB 113, **Computer Data Authentication**, May 1985.

c. FIPS PUB 140-1, **Security Requirements for Cryptographic Modules**, Jan. 1994

d. FIPS PUB 140-2, **Security requirements for Cryptographic Modules**, May 2001.

e. FIPS PUB 180-2, **Secure Hash Standard (SHS)**, August 2002.

f. FIPS PUB 181, **Automated Password Generator**, October 1993.

g. FIPS PUB 185, **Escrowed Encryption Standard**, February 1994.

h. FIPS PUB 186-2, **Digital Signature Standard (DSS)**, October 2001.

i. FIPS PUB 188, **Standard Security Labels for Information Transfer**, September 1994.

j. FIPS PUB 190, **Guideline for the Use of Advanced Authentication Technology Alternatives**, September 1994.

k. FIPS PUB 191, **Guideline for the Analysis of Local Area Network Security**, Nov. 9, 1994.

l. FIPS PUB 196, **Entity Authentication Using Public Key Cryptography**, February 1997.

m. FIPS PUB 197, **Advanced Encryption Standard Federal Agencies**, November 2001.

n. FIPS PUB 198, **The Keyed-Hash Message Authentication Code (HMAC)**, March 2002. This document was updated on April 8, 2002.

o. FIPS PUB 199, **Standards for Security Categorization of Federal Information and Information Systems**, February 2004.

p. *FIPS PUB 201-1, **Personal Identity Verification (PIV) of Federal Employees and Contractors**, June 26, 2006.

545.4.1.9 Office of Management and Budget (OMB)

a. OMB Circular No. A-130, **Revised (Transmittal Memorandum No. 4), Management of Federal Information Resources**, November 30, 2000. (Authority)

b. OMB Circular No. A-123, **Management Accountability and Control**, June 21, 1995.

c. OMB Memorandum 99-18, **Privacy Policies on Federal Web Sites**, June 2, 1999.

d. OMB Memorandum M-00-07, **Incorporating and Funding Security in Information Systems Investments**, February 28, 2000.

e. OMB Memorandum 00-13, **Privacy Policies and Data Collection on Federal Web Sites**, June 22, 2000.

f. OMB Memorandum M-00-15, **Guidance on Implementing the Electronic Signatures in Global and National Commerce Act**, September 2000.

g. OMB Memorandum M-01-08, **Guidance on Implementing the Government Information Security Reform Act**, January 16, 2001.

h. OMB Memorandum M-01-24, **Reporting Instructions for the Government Information Security Reform Act**, June 22, 2001.

i. OMB Memorandum M-02-01, **Guidance for Preparing and Submitting Security Plans of Action and Milestones**, October 17, 2001. (Authority)

j. OMB Memorandum M-03-22 **Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002**, 30 September 2003. (Authority)

k. OMB Memorandum M-04-04, **E-authentication Guidance for Federal Agencies**, December 2003.

l. OMB Memorandum M-04-25, **Reporting Instructions for the FISMA**, August 2004.

m. OMB Memorandum M-05-04, **Policies for Federal Agency Public Websites**, December 2004.

n. OMB Memorandum M-05-5, **Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services**, December 2004.

o. OMB Memorandum M-05-08, **Designation of Senior Agency Officials for Privacy**, February 2005.

p. OMB Memorandum M-05-15, **FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management**, June 2005.

545.4.1.10 Presidential Memorandums

a. **Directive to Develop Interagency Disability Web Site**, August 28, 2002.

b. **Electronic Government's Role in Implementing the President's Management Agenda**, July 10, 2002.

c. **Implementing Government Reform**, July 11, 2001.

d. **Action by Federal Agencies to Safeguard Against Internet Attacks**, March 3, 2000.

e. **Electronic Government**, December 17, 1999.

f. **Electronic Commerce Successes and Further Work**, November 30, 1998.

g. **Privacy and Personal Information & Federal Records** (Filed with Privacy Act Law), May 14, 1998.

h. **Electronic Commerce**, July 1, 1997

545.4.2 Internal Mandatory References

Effective Date: 07/25/2005

a. **ADS 502, The USAID Records Management Program**

b. **ADS 507, Freedom of Information Act (FOIA)**

c. **ADS 508, Privacy Act - 1974**

d. **ADS 509, Creating, Altering, or Terminating a System of Records (Records Pertaining to Individuals)**

e. **ADS 541, Information Management**

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

g. **ADS 557, Public Information**

h. **ADS 558, Public Activity**

i. **ADS 559, Inquiries from the News Media**

j. **ADS 560, News Releases and Services**

k. **Business Continuity Planning Procedures and Guidelines**

l. **Computer Security User Account Management Procedures** (Reserved)

m. **Data Remanence Procedures**

n. **Disaster Recovery Planning Procedures and Guidelines**

o. **E-Mail Acceptable Usage Policy**

p. **Establishing System Security Level Procedures and Guidelines**

q. **Firewall Guidelines** (Reserved)

r. Incidence Response Guidance for Unclassified Information Systems [Note: This document is only available on the intranet. Please contact **ads@usaid.gov** if you need a copy.]

s. **Incident Identification and Reporting Procedures**

t. **Information Assurance Procedures**

u. **Internet Acceptable Usage Policy**

v. **Media Handling Procedures and Guidelines**

w. **Mobile Computing Standards and Guidelines**

x. **Password Creation Standards and Technical Controls**

y. **Patch Management Guidelines** (Reserved)

z. **Personnel Security Procedures** (Reserved)

aa. **Restricted Access Procedures and Guidelines**

bb. **Risk Assessment Guidelines**

cc. **Rules of Behavior for Executive Management**

dd. **Rules of Behavior for Functional Management**

ee. **Rules of Behavior for Information System Security Officers**

ff. **Rules of Behavior for System Administrators**

gg. **Rules of Behavior for Users**

hh. **Security Self-Assessment Guidelines** (Reserved)

ii. **Virus Detection Guidelines**

jj. **Wireless Access Standards and Guidelines**

545.4.3 Mandatory Forms
Effective Date: 07/25/2005

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

b. AID Form 545-3, **Unclassified Information System Compliance Review**

c. AID Form 545-5, **USAID Sensitive Data Nondisclosure Agreement**

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

e. AID Form 545-7, **USAID Computer System Access Request** (replaces AID Form 545-1 and 545-4). [Note: This document is only available on the intranet. Please contact **ads@usaid.gov** if you need a copy.]

545.5 ADDITIONAL HELP
Effective Date: 07/25/2005

a. **Warning Screen Messages Guidelines**

545.6 DEFINITIONS
Effective Date – 07/25/2005

The terms and definitions listed below have been incorporated into the ADS Glossary. See the **ADS Glossary** for all ADS terms and definitions.

802.11
Refers to a family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless network technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless

clients. The range between units can be a few meters to over 450 meters. The IEEE accepted the specification in 1997. (Chapter 545)

accreditation
Security accreditation is the official management decision given by a Designated Approving Authority (DAA) to authorize operation of an information system, and to explicitly accept the risk to agency operations, agency assets, or individuals based upon the agreed upon implementation of a prescribed set of security controls. (Chapter 545)

administrative sanctions
Corrective or preventative, often disciplinary in nature, actions taken as part of a response to an incident where policy, procedure, or rule of behavior has been violated. (Chapter 545)

agency personnel
Refers to any individual who is employed by USAID or one of its contractors. (Chapter 545)

audit
To conduct an independent review and examination of system records and activities. (Chapter 545)

authentication
(1) The verification of an individual's identity, a device, or other entity in a computer system as a prerequisite to allowing access to resources in a system, or

(2) The verification of the integrity of data being stored, transmitted, or otherwise exposed to possible unauthorized modification.
(Chapter 545)

availability
Assurance of timely and reliable access to, and use of, information. (Chapter 545)

awareness, training and education
Awareness activities increase staff understanding of the importance of security and the adverse consequences of its failure. Training activities teach staff the skills to enable them to perform their jobs more effectively. Educational activities are more in-depth than training. {Source: NIST SP 800-12} (Chapter 545)

automated information system (AIS)
All activities, information, and material formerly identified as automated data processing (ADP), automation, office information systems, word processing, computers, and telecommunications. Referred to as an information system. (Chapters 545, 562)

biometrics
A technology that uses behavioral or physiological characteristics to determine or verify a user's identity (e.g. hand geometry, retina scan, iris scan, fingerprints, voice print, etc.). (Chapter 545)

Bluetooth
This technology enables seamless voice and data connections between a wide range of devices through short-range digital two-way radio operating in the 2.4 GHz spectrum. It is an open specification for short-range communications of data and voice between both mobile and stationary devices. (Chapter 545)

business continuity plan (BCP)
An overview of the requirements for ensuring that USAID's critical business functions, which are handled by its information systems, remain uninterrupted through time. (Chapter 545)

change control board (CCB)
One of the teams that evaluates the impact of proposed changes to the USAID baseline configuration, and determines if, and when, the changes are to be implemented. (Chapter 545)

certification
The comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. {Source: NSTISSI No. 1000} (Chapter 545)

certification authority (CA)
The USAID official who certifies that a particular information system has completed the certification process and is ready for accreditation by the Designated Approving Authority (DAA). (Chapter 545)

Chief Information Security Officer (CISO)
The Information Systems Security Officer, appointed by the CIO, is charged with protecting all network and automated information processing systems for the Agency by issuing policy, guidelines, and other such direction. The CISO is the authority for all security matters where AIS are concerned. (Chapter 545)

compiler
A program that reads source code, translates it into machine language, and writes the machine language to binary (object) code that can be directly loaded and executed.

confidentiality
Assurance that information is held in confidence and protected from unauthorized disclosure. (Chapter 545)

confidential information
Information for which the unauthorized disclosure could reasonably be expected to cause damage to the national security, which the original classification authority is able to identify or describe. (Chapter 545)

configuration management
A discipline to ensure that the configuration of an item and its components is known and documented, and that any changes are controlled and tracked. (Chapter 545)

connection
A connection is any established communications path between two or more devices or services. (Chapter 545)

copyrighted materials
Materials that have had a copyright placed upon them. A copyright is the collection of rights relating to the reproduction, distribution, performance and so forth of original works. The copyright owner has the exclusive right to do, or allow others to do, the acts set out the owners copyright. (Chapter 545)

Critical threat post
A posting which is located in a region where local treats such as social, political and natural disaster are. (Chapter 545)

data remanence
The physical representation of data which remains after the information is deleted from any device. (Chapter 545)

debugger
This is a development or problem-solving tool that allows one to examine, in detail, the execution of software. (Chapter 545)

dedicated machine
A machine exclusively used for a single purpose which performs no other major function. (Chapter 545)

designated approving authority (DAA)
The senior management official who has the authority to authorize processing (accredit) an automated information system (major application or general support system) and accept the risk associated with the system. {Source: NIST SP 800-12} (Chapter 545)

development environment
This term refers to an isolated network, machine or other environment where development and testing takes place with out the possibility of harm to any production system.

disaster recovery plan (DRP)
An overview of the requirements necessary to ensure that USAID's critical business functions that are handled by its information systems are resumed and restored after a natural or man-made disaster occurs. (Chapter 545)

de-militarized zone (DMZ)
A small subnet that "sits" between a trusted internal network, such as a private local area network, and an untrusted external network, such as the Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as web servers, file servers, e-mail servers. The term comes from military use, meaning a buffer area between two enemies. (Chapter 545)

Dynamic Host Configuration Protocol (DHCP)
A protocol that allows client devices to request IP addresses from a DHCP server as needed.

encryption
This is act of transforming information into an unintelligible form, specifically to obscure its meaning or content. (Chapter 545)

Executive Management/Manager (EM)
Managers who establish overall goals, objectives and priorities in order to support USAID. (Chapter 545)

executive order (EO)
A rule or order having the force of law, issued by the President of the United States.

firewall
A system available in many configurations that provides the necessary isolation between trusted and untrusted environments. (Chapter 545)

Functional Management/Manager (FM)
Managers who are responsible for a program or function including the supporting computer system (e.g. procurement or payroll). Their responsibilities include providing for appropriate security, including management, operational and technical controls. (Chapter 545)

general support system (GSS)
An interconnected set of information resources under the same direct management control which share common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared

information processing service organization. {Source: NSTISSI No. 1000; cites also OMB A-130} (Chapter 545)

help desk
Staff tasked with responding to user problems or security incidents, and other support related roles. (Chapter 545)

identification
The association of some unique or at least useful label to a person or entity to ascertain their identity. Identification answers the question, "Who is this person or entity?" (Chapter 545)

inbound network traffic
The term that generally refers to network traffic that comes into a firewall or server from the Internet or a lesser trusted network. (Chapter 545)

incident handling
The capability to recognize, react and efficiently handle disruptions in business operations arising from malicious activity or other threats. (Chapter 545)

individual accountability
The principle requiring that individual users be held accountable for their actions, after being notified of the rules of behavior in the use of the system, and the penalties associated with violations of those rules. {Source: NIST 800-18} (Chapter 545)

Industry best practice
A best practice is a technique or methodology that, through experience and research, has proven to reliably lead to a desired result.

information assurance
Information assurance is a set of processes by which USAID's information systems are reviewed, tested and evaluated, and certified and accredited. Information assurance processes are required to ensure that the risk from operating each information system is minimized and acceptable before deployment, and is kept at a minimal level while the system is operational. (Chapter 545)

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. {Source: a variation of a term from NSTISSI 4009} (Chapters 502, 545, 552, 562, 620)

Information Systems Security Officer (ISSO)
Individual responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security

posture is maintained for an information system or program. {Source: NIST 800-37} (Chapter 545)

information technology (IT)
General term used to describe any equipment or interconnected system or subsystem of equipment that is used to produce, manipulate, store, communicate, or disseminate information. (Chapter 545)

integrity
The safeguarding of information, programs and interfaces from unauthorized modification or destruction. (Chapter 545)

intellectual property (IP)
Intangible property that is the result of intellectual effort and is legally protected. Intellectual property is protected by patents, trademarks, designs, copyright, and so on. (Chapter 545)

interim approval to operate (IATO)
Determination applied when a system does not meet the requirements stated in the System Security Authorization Agreement (SSAA), but mission criticality mandates the system become operational. {Source: NSTISSI No. 1000} (Chapter 545)

Internet
The collection of interconnected networks that connect computers around the world. (Chapter 545)

intranet
A private network belonging to USAID, which is separate from the Internet and accessible only by internal staff. (Chapter 545)

issue-specific policies
Address specific areas of relevance and concern to the Agency (e.g. e-mail, Internet connectivity, mobile device use). These policies span the entire Agency, and often contain position statements on technology. (Chapter 545)

least privilege
The principle requiring that each subject be granted the most restrictive set of privileges that still allows the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system (IS). (Chapter 545)

logical access controls
The means by which the ability to do something is explicitly enabled or restricted. (Chapter 545)

major application
An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the system in which they operate. {Source: OMB A-130} (Chapter 545)

managerial controls
Security methods that focus on mechanisms that are primarily implemented by management personnel. (Chapter 545)

media
A broad term that normally defines physical devices in all formats that store and communicate information. Some examples of media as they relate to computers are: CDRoms, tapes, diskettes, disk drives, memory sticks, and others. (Chapter 545)

need to know
The need for specific information not normally available with out justification and possibly authorization prior to the release of the information in question. (Chapter 545)

network
A group of computers and associated devices connected by communications facilities (both hardware and software) to share information and peripheral devices, such as printers and modems. (Chapter 545)

non-disclosure agreement
A legal contract between two parties which outlines confidential materials the parties wish to share with one another for certain purposes, but wish to restrict from generalized use.

operational controls
Security methods that focus on mechanisms that are primarily implemented and executed by people. {Source: NIST SP 800-18} (Chapter 545)

password
A unique string of characters that a user must type to gain access to a computer system. (Chapter 545)

personnel
The term “personnel” refers to any USAID employee, contractor, or any other individual providing services to USAID, directly or indirectly. Personnel may or may not be authorized to use USAID information systems. (Chapter 545)

plan
An overview of the requirements for completing a task. (Chapter 545)

policy
A high-level statement of goals and objectives for USAID's information systems security. (Chapter 545)

port
Used in this document to denote a place where one might connect a computer to a network.

privacy impact assessment
The Privacy Impact Assessment (PIA) is a process used to evaluate privacy in information systems. It is basically a checklist or tool to ensure that new or modified electronic collections of information on individuals are evaluated for privacy risks and will comply with federal guidelines regarding privacy issues as they relate to information systems. (Chapter 545)

procedure
A description of steps that must be completed in a specific order, to accomplish a task. (Chapter 545)

program management
Used in the context of this document, is the process of creating and managing the information security program, including policies and enforcement guidelines that are designed to protect USAID's voice/data network equipment, computers and information. (Chapter 545)

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, 629)

program-specific policies
Define the information security program (infrastructure), set agency-specific strategic direction, assign responsibility within the infrastructure, and address compliance with policy. These policies span USAID. (Chapter 545)

public area
Any space or area that is open to the general public. (Chapter 545)

risk
A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact. {Source: NSTISSI No. 1000} (Chapter 545)

risk assessment
The process of analyzing threats to and vulnerabilities of an information system, and the potential impact the loss of information or capabilities of a system would have. The resulting analysis is used as a basis for identifying appropriate and cost-effective countermeasures. {Source: NSTISSI No. 1000} (Chapter 545)

risk management
The process concerned with the identification, mitigation and elimination of threats to, and vulnerabilities of, an information system to a level commensurate with the value of the assets protected. {Source: NSTISSI No. 1000} (Chapter 545)

role
These are the actions and activities assigned to, or required of, a person in a specific position or job. (Chapter 545)

rules of behavior (ROB)
Rules that clearly delineate responsibilities and expected behavior of all individuals with access to a system. {Source: NIST SP 800-12} (Chapter 545)

security incident
An adverse event that results from malicious activity, or the threat of such an event occurring. (Chapter 545)

security level
The security level for an information system is defined by the potential impact on a system should a breach in security occur. {Sources: NIST SP 800-60, FIPS 199} (Chapter 545)

security test and evaluation (ST&E)
The examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system. {Source: NSTISSI No. 1000} (Chapter 545)

sensitive but unclassified information (SBU)
SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set fourth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information, (TL;DS-61;10-01-199), 12 FAM 541 Scope, (TL;DS-46;05-26-1995).

SBU information includes, but is not limited to:

- Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations; and

- Information offered under conditions of confidentiality which arises in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers. (Chapter 545)

separation of duties
A requirement that two more individuals are needed to complete a process. This ensures that no single individual has complete control over process execution. (Chapter 545)

staff
The term "staff" refers to any USAID employee, contractor, or any other individual providing services to USAID, directly or indirectly. Staff may or may not be authorized to use USAID information systems. (Chapter 545)

system
Refers to any information system or application, and may be used to designate both the hardware and software that comprise it. (Chapter 545)

System Administrator (SA)
Are typically responsible for the technical security, installation, configuration, and maintenance of both the software and associated hardware and have elevated system privileges. (Chapter 545)

system development life cycle planning (SDLC)
Is the process of developing information systems through investigation, analysis, design, implementation, and maintenance. (Chapter 545)

System Owner (SO)
Individual responsible for daily program and operational management of their specific USAID system. System Owners are responsible for ensuring that a security plan is prepared, implementing the plan and monitoring its effectiveness. (Chapter 545)

system security authorization agreement (SSAA)
The SSAA is a document required to do Certification &Accreditation (C&A). It is a representation of a system through which the C&A process is applied. It identifies and describes the system, security and operational requirements, roles and responsibilities, level of effort, and resources required. (Chapter 545)

system security plan (SSP)
An overview of the security requirements of the computer system and the controls in place or planned to meet those requirements. The SSP delineates responsibilities and expected behavior of all individuals who access the computer system. (Chapter 545)

system-specific policies
Apply to single systems, they often address the context for meeting that system's particular security objectives. (Chapter 545)

technical controls
Hardware and software controls used to provide automated protection to the system or applications. {Source: NIST 800-18} (Chapter 545)

threat
Any circumstance or event with the potential to adversely impact agency operations (including mission functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. {Source: NIST 800-37} (Chapter 545)

token (specifically: authentication token)
A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. (Chapter 545)

traceability
The ability to trace a policy to or from a rule of behavior. (Chapter 545)

Trojan or Trojan horse
When referring to software a Trojan (also called a Trojan horse) is a seemingly harmless software program that contains harmful or malicious code. Trojans can allow hackers to open backdoors on your system, giving them access to your files and even network connectivity. (Chapter 545)

unclassified information
Information that has not been determined, pursuant to EO 12958 or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified. (source: NTISSI 4009). A category of information that includes both SBU and non-sensitive information and materials which, at a minimum, must be safeguarded against tampering, destruction, or loss. SBU information and materials must also be afforded additional protections commensurate with the sensitivity level of the data involved. (Chapters 545, 552)

USAID system
A system funded and operated by or for the Agency, and located in space owned or directly leased by the Agency. (Chapter 545)

User
The terms “user” or “users” refers to any USAID employee or contractor, or other individual, with authorized access to USAID’s information systems. A user can also be someone who uses information processed by USAID’s information systems. (Chapter 545)

user classifications
NIST SP 800-16 defines five user classifications: Users, Systems Administrators, Information System Security Officers, Functional Management/Managers, and Executive Management/Managers. A user classification is a group of users with similar roles and responsibilities. (Chapter 545)

validation
The process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for use of an information system. {Source: NSTISSI No. 1000} (Chapter 545)

verification
The process of comparing two levels of an information system specification for proper correspondence, e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code. {Source: NSTISSI No. 1000} (Chapter 545)

virus
Typically, a small computer program that has the capability to self execute and replicate on the infected machine as well as other machines. Viruses can cause damage to data, make computer(s) crash, display messages, provide backdoors, or any number of other things. Viruses, as opposed to worms, are meant to replicate themselves on a given system. The term virus is sometimes used to generically describe not only viruses, but also to include worms and Trojans collectively. (Chapter 545)

visitor
This is an individual, who is not authorized to access the USAID facility, to which they have gained access, and who is being escorted by an authorized individual. (Chapter 545)

vulnerability
Weaknesses in an information system, system security procedure, internal control, or implementation that could be exploited. {Source: NSTISSI No. 1000} (Chapter 545)

vulnerability assessment
A systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (Source: NSTISSI No. 1000) (Chapter 545)

waiver
The written permission required to eliminate the requirements of a specific policy. Authorized individuals may grant waivers to meet specific business needs. (Chapter 545)

worm
A computer program which replicates itself and is self-propagating across networks. Worms, as opposed to viruses, are meant to spawn in network environments. Worms usually are designed to slow down a network or even crash it. (Chapter 545)

545_061206_w061306_cd44