ADS Chapter 545

Information Systems Security

Full Revision Date: 11/09/2012
Responsible Office: M/DCIO
File Name: 545_110912

Functional Series 500 – Management Services
ADS 545 – Information Systems Security
POCs for ADS 545: Michael Wilsher, (703) 666-1449, MWilsher@usaid.gov and Sharon Robinson, (703) 666-5657, shrobinson@usaid.gov

This chapter has been revised in its entirety.

Table of Contents

545.1 OVERVIEW 5

545.2 PRIMARY RESPONSIBILITIES 7

545.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES 12

545.3.1 Waivers and Exceptions 12

545.3.2 Changes to Policy 14

545.3.3 Management Policies 14
545.3.3.1 Broad Organizational Policies 14
545.3.3.2 Security Program Management 16
545.3.3.3 Security Planning 18
545.3.3.4 Capital Planning and Investment Control 19
545.3.3.5 Contractors and Outsourced Operations 20
545.3.3.6 Performance Measures and Metrics 21
545.3.3.7 Contingency Planning 21
545.3.3.8 System and Services Acquisition 24
545.3.3.9 System Development Life Cycle 26
545.3.3.10 Configuration Management 27
545.3.3.11 Risk Management 29
545.3.3.12 Security Assessment and Authorization 30
545.3.3.13 Information Security Review and Assistance 33
545.3.3.14 Information Security Awareness Communications 34
545.3.3.15 Information Security Policy Violation and Disciplinary Action 34
545.3.3.16 Required Reporting 35
545.3.3.17 Privacy and Data Security 35
545.3.3.18 E-Authentication 40
545.3.3.19 CFO Designated Systems 41
545.3.3.20 Social Media and Social Networking 43

545.3.4 Operational Policies 45
545.3.4.1 Personnel Security 45

Text highlighted in yellow indicates that the material is new or substantively revised.

545.3.4.2 Physical and Environmental Protection 49
545.3.4.3 Media Controls 52
545.3.4.4 Video and Voice Communications Security 54
545.3.4.5 Data Communications 55
545.3.4.6 Wireless Communications 56
545.3.4.7 Overseas Communications 60
545.3.4.8 System Maintenance 60
545.3.4.9 Equipment 62
545.3.4.10 Agency Information Security Operations 65
545.3.4.11 Incident Management and Response 66
545.3.4.12 Documentation 68
545.3.4.13 Converging Technologies 69

545.3.5 Technical Policies 70
545.3.5.1 Identification and Authentication 70
545.3.5.2 Access Control 72
545.3.5.3 Auditing and Accountability 75
545.3.5.4 System and Communications Protection 77
545.3.5.5 Cryptography 85
545.3.5.6 System and Information Integrity 88
545.3.5.7 Product Assurance 90

545.3.6 USAID-Specific And Other Policies 91
545.3.6.1 Pilots, Prototypes, Proof of Concepts 91
545.3.6.2 Critical Threat Posts 91
545.3.6.3 Internet and Intranet Usage 92
545.3.6.4 Internet Radio 92
545.3.6.5 Instant Messaging 93
545.3.6.6 Mobile Computing Devices 93
545.3.6.7 Information Sharing 94
545.3.6.8 Intellectual Property Management 96
545.3.6.9 Third-Party Web Sites 97
545.3.6.10 Cloud Computing 98
545.3.6.11 Open Source 100
545.3.6.12 Shareware 100
545.3.6.13 Freeware 101
545.3.6.14 Remote Control Software 101
545.3.6.15 Collaboration Software 101
545.3.6.16 File-Sharing Software 102

545.4 MANDATORY REFERENCES 102

545.4.1 External Mandatory References 102

Text highlighted in yellow indicates that the material is new or substantively revised.

545.4.2 Internal Mandatory References 112

545.4.3 Mandatory Forms 115

545.5 ADDITIONAL HELP 115

545.6 DEFINITIONS 115

Chapter 545 – Information Systems Security

545.1 OVERVIEW

Effective Date: 11/09/2012

This chapter details the information security policies, consistent with federal regulations, mandates, and directives, which serve as the highest-level policy guidance for USAID's information systems, data, and other systems that process and/or store Agency information. ADS Chapter 545 applies to all Agency staff and others who use systems attached to networks managed by USAID.

The Office of Management and Budget (OMB) Circular **OMB A-130, Management of Federal Information Resources** requires that USAID provide "adequate security" for its information systems and data. Adequate security is 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."

Federal mandates also require that Agency information systems and applications provide information assurance, to include confidentiality, integrity, and availability, for Agency assets and operations.

This chapter does not apply to classified systems, however. For information on classified information systems processing, see **ADS 552, Classified Information Systems Security**.

NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, requires three security policy types as follows:

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 are Agency wide.

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 policies are Agency wide and often contain position statements on technology.

The **Federal Information Security Management Act of 2002** (FISMA) requires that each Federal agency must implement an agency-wide information security program to protect its operations and assets.

Federal mandates also require that agency information systems and applications provide information assurance to agency assets and operations. This means "appropriate confidentiality, integrity and availability."

The National Institute of Standards and Technology (NIST) Special Publication (SP) **SP 800-12, An Introduction to Computer Security** requires traceability from federal mandates to this chapter and its supporting documents such as plans, procedures, and checklists. Mandates in addition require security controls on information systems. They must include specified cost-effective management, operational, and technical controls, according to **NIST SP 800-12**. Controls reduce risk so that information systems operate safely, effectively, and economically.

NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations describes how to select security controls for information systems, and provides a baseline of security controls. This publication also categorizes security controls into Family and Class and attaches an identifier to each. The following table indicates Identifier, Family, and Class of security controls described in this chapter, and assigned to each section:

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

The Federal Information Processing Standards (FIPS) **FIPS 200, Minimum Security Requirements for Federal Information and Information Systems** identifies minimum security requirements for all components of information systems which process, store, or transmit Agency information.

Throughout this chapter are hyperlinks to other ADS chapters and **MANDATORY REFERENCES** (external and internal). They provide more information on many of the topics covered here. Both external and Internal mandatory references include (1) policies that the Agency has identified as necessary for the proper conduct of its business and (2) required procedures which identify more detailed courses of action that must be followed. Every USAID employee must comply with mandatory guidance. Acronyms, which appear throughout this chapter, are defined at first use and in Section 545.6 DEFINITIONS. Acronyms for security controls are defined in the table on the previous page.

The following standard terms appear throughout this chapter:

System refers to any USAID information system or application including the hardware and software in the information system or application.

Employee includes all USAID U.S. citizen direct-hire personnel, Personal Service Contractors (PSC) and Participating Agency Staff (PASA).

Staff refers to any USAID employee, contractor, Foreign Service National (FSN) or any other individual providing services to USAID, directly or indirectly. Staff may or may not be authorized to use USAID information systems.

User(s) refers to any staff member with authorized access to USAID's information systems. A user can also be someone who uses information processed by USAID's information systems and may have no access to USAID's information systems.

USAID Policy and Rules of Behavior (ROB) apply to all Agency Staff, including those who telework, regardless of how they interact with or access Agency information systems.

Agency refers to USAID.

545.2 PRIMARY RESPONSIBILITIES

Effective Date: 11/09/2012

This section describes the primary responsibilities for information system security. Applicable security controls, as identified in **NIST SP 800-53, Rev. 3** include PL, PM, and CA.

Governmental offices and employees (United States Direct Hires) bear primary responsibilities for information systems security. Although contractors, PSCs, and others working on behalf of USAID may support security functions, a USAID employee must always be designated as the responsible agent for all security requirements and

functions. Unless explicitly stated otherwise, government employees must fill all primary information security roles.

Primary Information Security Program Roles: Designated staff play a major role in the management, planning, and implementation of information security requirements.

Delegation of Roles: At the discretion of senior agency officials, certain USAID Security Authorization roles may be delegated (e.g., role representatives) and, if so, must be documented. Bureau officials may appoint qualified individuals to perform activities associated with any USAID Security Authorization role with the exception of the Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Privacy Officer (CPO), and Authorizing Official (AO).

The following sections describe the roles and responsibilities of key participants involved in an organization's risk management process as noted in NIST SP 800-37 (rev. 1) Guide to Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Appendix D, which contains more detail.

a. The Head of the Agency, the **Administrator,** is the highest-level senior official or executive within USAID with the overall responsibility to provide information security protections. The Administrator establishes:

(1) The organizational commitment to information security and the actions required to effectively manage risk and protect the core missions and business functions being carried out by the organization.

(2) The appropriate accountability for information security and provides active support and oversight of monitoring and improvement for the information security program.

(3) Senior leadership commitment to information security establishes a level of due diligence within USAID that promotes a climate for mission and business success.

b. The **Chief Information Officer (CIO), Bureau for Management, Office of the Chief Information Officer (M/CIO),** is responsible for the appropriate allocation of resources, based on Agency priorities, dedicated to the protection of the information systems supporting the organization's missions and business functions. The CIO also designates the senior information security officer or Chief Information Security Officer (CISO).

c. The Agency's senior information security official is the **Chief Information Security Officer (CISO).** The CISO's duties include: (i) carrying out the CIO security responsibilities under the Federal Information Security Management Act (FISMA); and (ii) serving as the primary liaison for the CIO to the organization's AOs, information SO, common control providers, and Information System Security Officers (ISSOs). The CISO (or supporting staff members) may also serve as AO designated representatives or security control assessors.

d. The **Chief Privacy Officer (CPO**) is responsible for maintaining oversight of the USAID Privacy Program to ensure that it is in compliance with all applicable statutory and regulatory guidance.

e. The **Risk Executive** is an individual or group within the Agency that helps to ensure that disk-related considerations for individual information systems, to include authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the Agency in carrying out its core missions and business functions.

f. The **Information Owner/Steward** is an Agency official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. The owner/steward of the information processed, stored, or transmitted by an information system may or may not be the same as the information system owner (SO).

g. The **Authorizing Official (AO)** is a senior executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations and assets, individuals, other organizations.

AOs can deny authorization to operate an information system or if the system is operational, halt operations, if unacceptable risks exist. AOs coordinate their activities with the risk executive (function), CIO, senior information security officer, common control providers, information SO, ISSOs, security control assessors, and other interested parties during the security authorization process.

h. The **Authorizing Official Designated Representative** is an Agency official who acts on behalf of an AO to coordinate and conduct the required day-to-day activities associated with the security authorization process.

The only activity that cannot be delegated to the designated representative by the AO is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk to Agency operations and assets, individuals, other organizations).

i. The **Common Control Provider** is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems). Common control providers are responsible for:

- Documenting the organization-identified common controls in a security plan (or equivalent document prescribed by the organization);
- Ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization;
- Documenting assessment findings in a security assessment report; and
- Producing a Plan of Action and Milestones (POA&M) for all controls having weaknesses or deficiencies. Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) is made available to information SO inheriting those controls after the information is reviewed and approved by the senior official or executive with oversight responsibility for those controls.

j. The **Information System Owner (SO)** is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The information SO is responsible for addressing the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or Agency requirements) and for ensuring compliance with information security requirements.

In coordination with the Information System Security Officer (ISSO), the information SO is responsible for the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls. In coordination with the information owner/steward, the information SO is also responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training, e.g., instruction in ROB.

k. The **Information System Security Officer (ISSO)** is an individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the information SO. The ISSO also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The ISSO has the detailed knowledge and expertise required to manage the security aspects of an information system and, in

many organizations, is assigned responsibility for the day-to-day security operations of a system.

l. The **Information Security Architect** is an individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.

m. The **Information System Security Engineer** is an individual, group, or organization responsible for conducting information system security engineering activities. Information system security engineers are an integral part of the development team (e.g., integrated project team) designing and developing organizational information systems or upgrading legacy systems.

n. The **Security Control Assessor** is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system.

Security control assessors also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities.

Additional Roles:

- **System Administrators** (**SA)**. A subclass of users, the SA role requires elevated privileges for the USAID network or a specific system. SAs are able to perform higher-order tasks, including technical operations prohibited for other general users.

- **Functional or Program Managers (PM)**. A subclass of users, this role requires elevated privileges, including responsibilities for a daily program and operational management of their specific USAID system (including the USAID network).

- **Executive Managers (EM)**. A subclass of users, this role requires the EM to manage and oversee USAID and its Missions.

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

545.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 11/09/2012

This section contains USAID's information system security policy directives and references to required procedures. Information security policies delineate the security management structure and foundation to measure progress and compliance. Policies in this document are organized under three areas as follows:

- Management Controls – Focus on managing both the system information security controls and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.

- Operational Controls – Focus on mechanisms primarily implemented and executed by people. These controls are designed to improve the security of a particular system or group of systems and often rely on management and technical controls.

- Technical Controls – Focus on security controls executed by information systems. These controls provide automated protection from unauthorized access or misuse. They facilitate detection of security violations and support security requirements for applications and data.

These policies are maintained by the CISO and may be altered to comply with federal regulations, mandates, and directives by way of periodic updates and/or Agency Notices, as required, in order to maintain the security of the Agency's information security profile.

545.3.1 Waivers and Exceptions

Effective Date: 11/09/2012

Information system(s) that do not fully comply with policy requirements due to a system weakness or need for a permanent exception to USAID policy will require a waiver/exception request from any portion of these policy requirements. Applicable controls include PL, PM, CA, and CM.

A waiver is the written permission required to temporarily eliminate the requirements of a specific policy or control. An exception is an authorization to proceed outside of policy when certain conditions apply. Authorized individuals (the CIO and CISO) may grant waivers and exceptions to meet specific business needs.

Exceptions are generally based on detrimental impact to mission, excessive costs, and/or clearly documented end-of-platform life for non-essential systems. Typical

exceptions also include commercial-off-the-shelf (COTS) products that cannot be configured to support the control requirements.

Waivers can be granted for a period up to six (6) months, and may be granted only one six-month extension. Exceptions are long term up to thirty-six (36) months (unless authorized longer by the CIO and CISO). Exceptions are issued when systems cannot be brought into compliance due to the issues mentioned in the paragraph above.

SOs may submit an exception request to the CISO through the system ISSO. If the deficiency or weakness exists in a financial system, the CFO must also approve the waiver request before sending to the CISO. If the deficiency or weakness exists in a Privacy system, the CPO must also approve the waiver request before sending to the CISO. If the exception is not authorized in writing the System must be decommissioned.

SOs may request waivers to, or exceptions from, any portion of this policy, for up to six (6) months, if they are unable to fully comply with policy requirements. One (1) six-month extension may be granted.

The CISO may issue waivers against USAID policy, where permissible by Federal regulation. The supporting documentation for waivers or exceptions must include at a minimum the following:

- System name,
- Specific conditions that necessitate the waiver,
- Specific policy being waived or excepted,
- Risk assumed with accepting the conditions of the waiver/exception,
- Waiver limitations,
- Risk mitigations or compensating controls,
- Rationale justifying a decision to waive policy,
- Time frame that the waiver remains effective, and
- POA&M for bringing the system or program into compliance.

Requests submitted without sufficient information will be returned for clarification prior to issuing a decision. In all cases waiver requests should be for an appropriate period based on a reasonable remediation strategy.

545.3.2 Changes to Policy
Effective Date: 11/09/2012

Requests for clarification and/or interpretation of this policy may be submitted to the CISO at **isso@usaid.gov.** Applicable controls include PL.

545.3.3 Management Policies
Effective Date: 11/09//2012

Management policies describe 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.

Management policies specifically address the information security program management, the required security planning for information systems, the required risk assessments before acquiring and deploying information systems, information system acquisition requirements, and certification and authorization of information systems.

545.3.3.1 Broad Organizational Policies
Effective Date: 11/09/2012

The following policies apply broadly to all Agency information systems as follows:

(1) Staff must adhere to the security policy contained in this chapter, and the plans, procedures, ROB, standards, checklists, and guidelines derived from policy.

(2) Staff must use information systems for USAID business or limited personal use as specified in the Agency acceptable use policy.

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

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

(5) Users have no reasonable expectation of privacy when using any USAID information system. USAID must protect the privacy of specific Personally Identifiable Information (PII) as required by law.

(6) Staff must make a reasonable effort to safeguard USAID information/data.

(7) Staff, ISSOs, SAs, 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.

(8) The CISO may monitor any device attached to the network at any time.

(9) The GSS ISSO must specify the points of control for Agency computing and telephony resources.

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

(11) The CIO, in cooperation with other Agency senior officials, is responsible for ensuring that every USAID computing resource (e.g., desktops, laptops, servers, and mobile electronic devices) is identified as an information system or as a part of an information system (major application or GSS).

(12) The SO or designee must develop and maintain a System Security Plan (SSP) for each information system.

(13) An ISSO must be designated for every information system and serve as the POC for all security matters related to that system.

(14) The CISO must ensure that all information systems comply with the USAID Enterprise Architecture (EA) and Security Architecture (SA) or issue a waiver for deficiencies. (The CIO may approve waivers for CISO owned systems.)

(15) The CISO must issue an Agency-wide information security policy, guidance, and architecture requirements for all USAID systems.

545.3.3.2 Security Program Management

Effective Date: 11/09/2012

Information Security program management covers a range of activities; it is based on the foundation of understanding information security risks, selecting and implementing controls commensurate with the risk, and ensuring that controls, once implemented, continue to operate effectively. The integration of identifying and assessing risks into the management procedures and the organizational culture is essential for security program management.

The following policy statements apply to Security Program Management:

(1) The CISO must develop and disseminate an organization-wide information security program plan that:

a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

b. Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan; and a determination of the risk to be incurred if the plan is implemented as intended;

c. Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

d. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations;

e. Reviews the organization-wide Information Security Program plan annually; and

f. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

(2) The Agency must appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. Applicable control includes PM-2.

(3) The Agency must ensure that all capital planning and investment requests include the resources needed to implement the Information Security Program and documents all exceptions to this requirement; employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and ensures that information security budget resources are available as planned. Applicable control includes PM-3.

(4) The CISO must implement a process for ensuring that POA&Ms for the security program and the associated organizational information systems are maintained and must document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations.

(5) The CISO must develop and maintain an inventory of its information systems.

(6) The CISO must develop, monitor, and report on the results of information security measures of performance.

(7) The CISO must develop enterprise architecture with consideration for information security and the resulting risk to Agency operations, Agency assets, individuals, other organizations.

(8) The CISO must address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

(9) The CISO must develop a comprehensive strategy to manage risk to agency operations and assets, individuals, and other organizations associated with the operation and use of information systems; and implements that strategy consistently across the Agency.

(10) The CISO must manage (i.e., document, track, and report) the security state of Agency information systems through security authorization processes; designate individuals to fulfill specific roles and responsibilities within the Agency risk management process; and fully integrate the security authorization processes into an Agency-wide risk management program.

(11) The CISO must establish information security processes with consideration for the Agency mission/business processes as well as the resulting risks to Agency operations, assets, individuals and other organizations.

(12) The CISO must determine information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

Refer to the **USAID FISMA Program Guide** for more information. [For a copy of this Guide, please contact the Information Assurance Division at **isso@usaid.gov**.]

545.3.3.3 Security Planning

Effective Date: 11/09/2012

Basic security management principles must be followed in order to ensure the security of information resources. These principles are applicable throughout the Agency and form the cornerstone of the USAID Information Security Program.

The following policy statements apply to security planning:

(1) The CISO must develop, disseminate, and review/update annually a security planning policy.

(2) SOs must coordinate with the CISO to document procedures to implement and enforce security planning policy and security planning associated controls.

(3) SOs must develop a functional architecture for the information system that identifies and maintains: external interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface; user roles and the access privileges assigned to each role; unique security requirements; types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders (EOs), directives, policies, regulations, standards, and guidance; and restoration priority of information or information system services.

(4) SOs must establish and make readily available to all information system users the rules that describe their responsibilities and expected behavior with regard to information and information system usage. SOs must

receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the ROB, before authorizing access to information and the information system.

(5) SOs must conduct a privacy impact assessment on the information system in accordance with OMB policy and USAID guidance.

(6) SOs must plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on Agency operations (i.e., mission, functions, image, and reputation), Agency assets, and individuals.

545.3.3.4 Capital Planning and Investment Control

Effective Date: 11/09/2012

Information security is a business driver. Risks found through security testing are ultimately business risks. Information security personnel should be involved, where necessary in the acquisition process, including drafting contracts for IT systems and services, and procurement documents. The **Federal Acquisition Regulation (FAR)** and **USAID ADS Acquisition and Assistance Series** provides additional information on these requirements.

The following policy statements apply to CPIC:

(1) SOs must include information security requirements in their CPIC business cases for the current budget year and for the future years for each USAID information system. For additional information on the CPIC process, see **NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process**, and **ADS 577, Information Technology Capital Planning and Investment Control**.

(2) SOs must ensure that information security requirements and POA&Ms are adequately funded, resourced, and documented in accordance with current OMB budgetary guidance.

(3) USAID approval/review boards must not approve any capital investment in which the information security requirements are not adequately defined and funded.

(4) The USAID CISO must perform security reviews for planned information system upgrades and acquisitions.

(5) SOs must ensure that information security requirements described in this chapter are included in the acquisition of all USAID systems and services used to input, process, store, display, or transmit sensitive information.

(6) Acquisition professionals in M/OAA must ensure the full enforcement of the **Federal Acquisition Regulation (FAR)** and **USAID ADS Acquisition and Assistance Series** provisions.

(7) Acquisition Professionals must follow the guidance in the **FAR Subpart 4.13** for personal identity verification for all contractor and subcontractor personnel when contract performance requires contractors to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

545.3.3.5 Contractors and Outsourced Operations

Effective Date: 11/09/2012

All Information Technology (IT) related Statements of Work (SOWs) and/or contracts must identify and document the specific security requirements for information system services and operations required of the contractor. The COR must ensure that contractor information system services and operations adhere to all applicable USAID information security policies. Applicable controls include SA and PM.

The following policy statements apply to contractors and outsourced operations:

(1) Requirements must address how sensitive information is to be handled and protected at contractor sites. This includes any information stored, processed, or transmitted using contractor information systems. Requirements must also include personnel background investigations and clearances as well as facility security requirements.

(2) The COR must ensure that SOWs and contracts include provisions stating that, upon the end of the contract, all information and information resources provided during the life of the contract are returned to the Agency; and that all USAID information has been purged from any contractor-owned system used to process USAID information.

(3) The COR must conduct reviews to ensure that contract language includes information security requirements.

(4) Security deficiencies in any outsourced operation must require creation of a POA&M at the appropriate level (Agency-wide, Program, or system).

545.3.3.6 Performance Measures and Metrics
Effective Date: 11/09/2012

The following policy statements apply to performance measures and metrics:

(1) The CISO must define performance measures to evaluate the effectiveness of the USAID Information Security Program.

(2) The CISO must collect OMB FISMA data from SOs and/or ISSOs at least quarterly and provide FISMA reports as required by OMB.

545.3.3.7 Contingency Planning
Effective Date: 11/09/2012

Contingency and continuity planning are management policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergency, system failure, or disaster.

Contingency planning is one component of a much broader emergency preparedness process that includes items such as business practices, operational continuity, and disaster recovery planning. Applicable controls include CP, AT, AC, CM.

Once critical systems are identified, continuity planning must address the following two complementary but different elements:

- Contingency Planning (CP), and
- Continuity of Operations Planning (COOP).

a. Contingency Planning (CP)

The following policy statements apply to contingency planning:

(1) The CIO must provide documented guidance, direction, and authority for a standard Agency-wide process for contingency planning for all USAID information systems requiring contingency planning.

(2) SOs must develop and document information system CPs for their programs, manage plan changes, and distribute copies of the plan to key contingency personnel.

(3) The CIO must ensure implementation of backup policy and procedures for every USAID information system.

(4) The CIO must ensure that each system has contingency capabilities commensurate with the available security objective. The minimum contingency capabilities for each impact level follow:

- High – System functions and information have a high priority for recovery after a short period of loss.
- Moderate – System functions and information have a moderate priority for recovery after a moderate period of loss.
- Low – System functions and information have a low priority for recovery after prolonged loss.

(5) SOs must develop and maintain CPs in accordance with the requirements of **FIPS 199, Standards for Security Categorization of Federal Information and Information Systems**. This guidance requires potential impact level for the availability security objective. These plans must be based on three essential phases: Activation/Notification, Recovery, and Reconstitution. SOs must review the CP for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

(6) The CIO must ensure that CP testing is performed in accordance with the availability security objective. The minimum contingency testing for each impact level follows:

- High – System recovery roles, responsibilities, procedures, and logistics in the CP must be used to recover from a simulated contingency event at the alternate processing site within a year prior to accreditation. The system recovery procedures in the CP must be used to simulate system recovery in a test facility at least annually.
- Moderate – System functions and information have a moderate priority for recovery after a moderate period of loss. The CP must be tested at least annually by reviewing and coordinating with organizational units or personnel responsible for plans within the CP. A tabletop exercise accomplishes the test.
- Low – CP contact information must be verified at least annually.

(7) The CIO must ensure that contingency training is performed in accordance with the availability security objective. The minimum contingency planning for each impact level follows:

- High – All staff involved in contingency planning efforts must be identified and trained in their contingency planning and implementation roles, responsibilities, procedures, System functions and information have a high priority for recovery after a short period of loss. This training may incorporate simulated events. Refresher training must be provided at least annually.

- Moderate – All system staff involved in contingency planning efforts must be trained. Refresher training must be provided at lest annually.

- Low – There is no training requirement.

(8) SOs must coordinate as appropriate CP testing and/or exercises with COOP-related plans for systems with Moderate and High availability, per the **FIPS 199** categorization.

b. Continuity of Operation Planning (COOP)

The following policy statements apply to COOP:

(1) An Agency-wide process for continuity planning must be used in order to ensure continuity of operations under all circumstances.

(2) SOs must develop, test, implement, and maintain comprehensive COOPs to ensure the continuity and recovery of essential USAID functionality.

(3) The CISO must ensure that all COOPs are tested and exercised annually.

(4) All CFO Designated Systems requiring high availability must be identified in COOP plans and exercises.

(5) All staff involved in COOP efforts must be identified and trained in the procedures and logistics of COOP development and implementation.

(6) To ensure that accounts can be created in the absence of the usual account approval authority, systems identified as critical assets must have provisions to allow the ISSO or other government employee to approve new user accounts as part of a COOP scenario.

(7) The CIO must create and maintain a list of mission-critical information systems in support of COOP.

(8) The CISO must ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.

545.3.3.8 System and Services Acquisition

Effective Date: 11/09/2012

A decision about the acquisition of a system or system components (i.e. hardware or software) may occur following the completion of a security risk assessment (See: 545.3.5.11 - Risk Management). A security risk assessment analyzes threats and vulnerabilities to an information system, along with the potential impact any loss of information or capability would have to a given system. System and Services Acquisition controls incorporate information security considerations when acquiring information systems, system components, or services.

The following policy statements apply to system and services acquisition:

(1) The CISO must develop, disseminate, and review/update annually a systems and services acquisition policy.

(2) SOs and responsible offices must coordinate to implement and enforce procedures to implement the system and services acquisition policy and associated system and services acquisition controls.

(3) SOs must include a determination of information security requirements for the information system in mission/business process planning.

(4) SOs must determine, document, and allocate the resources required to protect the information system as part of its capital planning and investment control process.

(5) SOs must establish a discrete line item for information security in organizational programming and budgeting documentation.

(6) SOs must include the following requirements and/or specifications, explicitly or in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

- Security functional requirements/specifications,

- Security-related documentation requirements, and
- Developmental- and evaluation-related assurance requirements.

(7) SOs must require that providers of external information system services comply with USAID information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. (External information systems services are not part of, connected to, operated or owned by the Agency. Generally these systems are under contract to, or funded by and operated on behalf of the Agency.)

(8) SOs must define and document government oversight and user roles and responsibilities with regard to external information system services.

(9) SOs must monitor security control compliance by external service providers.

(10) SOs must retain and protect as required, and make available to authorized staff, administrator documentation for the information system that describes: secure configuration, installation, and operation of the information system.

(11) SO's must retain, protect and make available administrator documentation for their system(s) that describe the secure configuration, installation, and operation of the information system to include the effective use and maintenance of security features/functions.

(12) SOs must retain and protect user documentation for their system. This documentation must include at least the following:

- User accessible security features/functions and their effective use,
- Methods for user interaction with the information system, and
- User responsibilities in maintaining the security of the information and information system.

(13) SOs must use software and associated documentation in accordance with contract agreements and copyright laws.

(14) SOs must employ tracking systems for software and associated documentation protected by quantity licenses to control copying and

distribution; and control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

(15) SOs must apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

(16) SOs must require that information system developers/integrators: perform configuration management during information system design, development, implementation, and operation; manage and control changes to the information system, Implement only organization-approved changes, and document approved changes to the information system; and track security flaws and flaw resolution.

(17) SOs must require that information system developers/integrators, in consultation with associated security staff (including security engineers): create and implement a security test and evaluation plan; implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and document the results of the security testing/evaluation and flaw remediation processes.

(18) SOs must manage the information system using a system development life cycle methodology. It must include information security considerations; define and document information system security roles and responsibilities throughout the system development life cycle; and identify individuals having information system security roles and responsibilities.

(19) SOs must enforce explicit rules governing the installation of software by users.

545.3.3.9 System Development Life Cycle

Effective Date: 11/09/2012

SDLC in systems engineering, information systems, and software engineering is a process of creating or altering information systems as well as the models and methodologies used to develop systems. Applicable controls include A and RA.

SDLC planning, in an information security context, is the standard SDLC process with emphasis on assessments and proper security controls. Federal requirements mandate identifying, implementing, and tracking information system security requirements prior to system implementation or operational deployment. This maintains system and software

security at system assessment level. For more information on SDLC project methodology, see the **USAID IT Project Governance Manual v 1.1**.

The following policy statements apply to SDLC:

(1) SOs must ensure the integration of system and software security into all SDLC phases.

(2) The CISO must provide, document, and maintain a framework and guidance for system and software security and data sensitivity assessments consistent with Federal regulation.

(3) The CISO must validate, for each USAID information system and system software, that the appropriate managerial, operational, and technical controls have been selected and implemented by SOs.

(4) SOs must ensure incorporation of security requirements for sensitive information systems into life-cycle documentation.

(5) The Program Manager must review, approve, and sign all custom-developed code prior to deployment into production environments. The Program Manager may delegate this authority to another USAID employee, but not to contractors, in writing.

545.3.3.10 Configuration Management

Effective Date: 11/09/2012

Configuration management (CM) refers to the configuration of all hardware and software elements within information systems and networks. CM within USAID consists of a multi-layered structure, which includes policy, procedures, processes, and compliance monitoring.

CM applies to all systems and subsystems of the USAID infrastructure, thereby ensuring implementation, and continuing life-cycle maintenance. CM begins with base-lining requirements documentation and ends with decommissioning items no longer used for production or support.

CM applies to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. A Change Management Process ensures the update of documentation associated with an approved change to a USAID system. This reflects the appropriate baseline, including an analysis of any potential security implications. Documentation must describe initial configuration in detail.

A robust, documented CM process must control subsequent changes. CM has security implications in three areas:

- **Ensuring** that the **configuration** of subordinate information system elements is consistent with the Security Authorization Process requirements of the parent system;

- **Ensuring** the **approval** of subsequent changes, including analysis of any potential security implications; and

- **Ensuring** proper **installation** of all recommended and approved security patches.

The following policy statements apply to CM:

(1) The CISO must develop, disseminate, and review/update annually a documented CM policy.

(2) SOs must document and enforce procedures to implement the CM policy and associated controls.

(3) SOs must develop and maintain a Configuration Management Plan (CMP) for each information system as part of its SSP.

(4) SOs must establish, document, implement, and enforce CM controls on all information systems and networks and address significant deficiencies as part of a POA&M.

(5) Security patches must be installed in accordance with configuration management plans and within the timeframe or direction stated within the **USAID Vulnerability Management Guide**. [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.]

(6) SOs must document the initial system configuration in detail and control all subsequent changes in accordance with the CM process.

(7) Workstations must be configured in accordance with **United States Government Configuration Baseline** (USGCB, formerly known as the Federal Desktop Core Configuration [FDCC]).

(8) The CISO must monitor USGCB (or Agency-approved USGCB variations) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool.

(9) The SO must request an exception for information systems using operating systems or applications, which are not hardened or do not follow configuration guidance identified in the **USAID Secure Baseline Configuration Guide**. [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.] Requests must include a proposed alternative secure configuration.

(10) SOs, when considering proposed changes, must ensure that CM processes for their systems reflect the results of a security impact analysis.

(11) SAs must configure servers to conform to internal server standards.

(12) SAs must place internet-accessible servers in a De-Militarized Zone (DMZ), (e.g., web, e-mail, etc.).

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

(14) SAs and the System ISSO must evaluate new servers and their interconnections for security risks.

545.3.3.11 Risk Management

Effective Date: 11/09/2012

The Risk Management process enables SOs to balance the operational and economic costs of protective measures. This balance improves mission capability by protecting the information systems and data that support their organization's missions.

The following policy statements apply to risk management:

(1) The CISO must develop, disseminate and review/update annually a risk assessment policy.

(2) The CISO must document and enforce procedures to implement the risk assessment policy.

(3) The CISO must establish a risk management program in accordance with **NIST SP 800-30, Risk Management Guide for Information Technology Systems** and other applicable Federal guidelines.

(4) The CISO must ensure a system risk assessment under any of the following conditions:

a. Annually;

b. When a sensitive system experiences high-impact weaknesses; and

c. When a sensitive system, its physical environments, interfaces, or user community, experiences a modification.

The risk assessment must consider the effects of the modifications on the system operational risk profile. There then must be an update to the system SSP and, if warranted by the results of the risk assessment, a system re-certification.

(5) The CISO must establish an independent Agency-wide Security Authorization program to ensure a consistent approach to testing the effectiveness of controls.

(6) Risk Executives or the CISO must review recommendations for risk determinations and risk acceptability and may recommend changes to the AO and CIO.

(7) The CIO must deploy an Agency-wide network vulnerability scanning program.

Note: Special rules apply to CFO Designated Systems. See Section 545.3.3.19, CFO Designated Systems, for additional information.

545.3.3.12 Security Assessment and Authorization

Effective Date: 11/09/2012

Upon acquiring or developing an information system, a Security Assessment and Authorization (A&A), formerly known as a Certification and Accreditation (C&A), is required to obtain an Authority to Operate (ATO) the system. An ATO must be granted prior to the deployment of the information system.

USAID periodically assesses the selection of security controls to determine their continued effectiveness in providing appropriate protection. The **USAID Security Authorization Process Guide** describes detailed processes governing the Security Authorization Process and system risk assessment. Detailed information for creating and managing Plans of Action and Milestones (POA&Ms) appears in the **USAID POA&M Process Guide**. Additional information may also be found in the **USAID FISMA Program Guide**. [For a copy of these guides, please contact the Information Assurance Division at **isso@usaid.gov**.] Applicable controls include PM, RA, and CA**.**

The following policy statements apply to security assessment and authorization:

(1) The CISO must develop, disseminate, and review/update annually documented security assessment and authorization policy and procedures for implementation of the policy.

(2) SOs must assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each USAID information system. SOs must apply **NIST SP 800-53, Rev. 3** controls as tailored by the CISO specific to the security objective at the determined impact level.

(3) SOs must implement **NIST SP 800-53, Rev.3**, security controls, using the methodology, based on the **FIPS 199** impact level set for each separate security objective (confidentiality, integrity, availability).

(4) SOs may pursue Type Security Authorization for information resources which meet one or more of the following conditions:

a. Are under the same direct management control;

b. Have the same function or mission objective, operating characteristics, and security needs;

c. Reside in the same general operating environment; and

d. In the case of a distributed system, reside in various locations with similar operating environments.

The Security Authorization Process, as defined by the CISO, must consist of the following:

a. A master Security Authorization Process package describing the common controls implemented across sites; and

b. Site-specific controls and unique requirements that have been implemented at the individual sites.

(5) The AO or SO for a system must be identified in Cyber Security Assessment Management (CSAM) or other CISO-approved automated tool. The CIO serves as the AO whenever the SO or an appropriate Agency official has not been named as the AO.

(6) For all information systems, the CISO must ensure a formal assessment that fully evaluates their management, operational, and technical security controls.

(7) The assessment must be a part of, and in support of, the accreditation process. It must determine the extent to which a particular design and implementation plan meets the CISO-required set of security controls. An information system categorized as a moderate or high must be assessed by an independent assessor.

(8) The CISO must ensure that a risk assessment is conducted whenever any modifications are made to sensitive information systems, networks, or to their physical environments, interfaces, or user community. SSPs must be updated and re-authorizations conducted if warranted.

(9) SOs must accredit systems at initial operating capability and every three (3) years thereafter, or whenever a major change occurs, whichever occurs first. A major change includes, but is not limited to, full version changes for software or operating systems; physical environment changes; user community or other changes that might impact the security posture of the network, system or information.

(10) The CISO may grant a Restrictive Authorization to Operate (RATO) for systems that are undergoing development testing or are in a prototype phase of development. A RATO is a legally binding written permission to conduct activities but under certain restrictions. RATOs must not be used for operational systems. The CISO may grant an RATO for a maximum period of 6 (six) months and may grant one (1) six (6)-month extension. Systems under a RATO must not process sensitive information but may attach to system networks for testing. Interim Authorizations to Operate (IATO) are not granted by the Agency and are not recognized by OMB.

(11) Systems must not be deployed as an operational system until they have received an ATO certified by the CISO and signed by the SO or AO.

(12) The CISO must specify tools, techniques, and methodologies used to certify and accredit USAID information systems, report and manage FISMA data, and document and maintain POA&Ms.

(13) All USAID systems must be accredited using the automated tools approved by the CISO.

(14) The CISO must maintain a repository for all Security Authorization Process documentation and modifications.

(15) The CISO must establish processes to ensure consistent Security Authorization across all USAID systems.

(16) SOs must use the POA&M process to manage vulnerabilities, correct deficiencies in security controls, and remediate weaknesses in SSPs.

(17) The AO must formally assume responsibility for operating an information system at an acceptable level of risk. System operation with sensitive information is prohibited without an ATO.

(18) ATOs must only be provided for systems that fully comply with policy or have been granted appropriate exceptions or waivers.

(19) The CIO may revoke any ATO of any USAID information system.

(20) The CISO must assign common controls to share controls between systems. The authorization package of those common controls must be shared with those operating under them.

545.3.3.13 Information Security Review and Assistance

Effective Date: 11/09/2012

Security review and assistance are required to ensure that SOs comply with Agency and federal policy and guidance. It is the responsibility of those with primary security roles to assist with compliance issues as required. Applicable controls include PL, CA and PM.

The following policy statements apply to information security review and assistance:

(1) SOs must submit their information security policies to the CISO for review.

(2) SOs must conduct their security reviews in accordance with **FIPS 200** and **NIST SP 800-53, Rev. 3** for specification of security controls. **NIST SP 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations**, will be used for assessing the effectiveness of security controls and for periodic FISMA reporting.

(3) The CISO must conduct information security review and assistance throughout the Agency in order to monitor the effectiveness of information security.

545.3.3.14 Information Security Awareness Communications

Effective Date: 11/09/2012

Working groups and other forums throughout the federal government representing various functional areas convene on a regular basis. These entities are responsible for establishing significant security requirements, promoting communications between federal organizations, and developing security best practices. USAID CISO must remain engaged with such entities to ensure awareness of security issues and effectively communicate such issues to USAID staff. Applicable control includes AT.

The following policy statements apply to information security awareness and communications:

(1) The CISO must ensure that security-related decisions and information, including updates to the ADS 545 and other security-related policies, are distributed to the SOs, ISSOs and other appropriate persons.

(2) All staff must abide by the security training requirements listed in the Information Security Awareness, Training, and Education section of this policy - 545.3.4.1(e).

545.3.3.15 Information Security Policy Violation and Disciplinary Action

Effective Date: 11/09/2012

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 ROB derived from them, may be subject to the full range of administrative disciplinary actions as defined in **ADS 485, Disciplinary Action - Foreign Service** or **ADS 487, Disciplinary and Adverse Actions Based Upon Misconduct - Civil Service**, 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.

545.3.3.16 Required Reporting
Effective Date: 11/09/2012

FISMA requires reporting the status of the USAID Information Security Program to OMB on a recurring basis. Applicable control includes CA.

The following policy statements apply to required reporting:

(1) The CISO must collect and submit quarterly and annual information security program status data as required by FISMA.

(2) Only automated tools approved for use by the CISO must be used for collecting required reporting information.

545.3.3.17 Privacy and Data Security
Effective Date: 11/09/2012

The USAID Privacy Office is responsible for privacy compliance across the Agency. This includes assuring that technologies used by the Agency sustain, and do not erode, privacy provisions as specified by the Privacy Act of 1974. The USAID CPO has exclusive jurisdiction over the development of policy relating to Personally Identifiable Information (PII). For additional information concerning privacy-related policy, contact the CPO (**privacy@usaid.gov**) or refer to **ADS 508, The USAID Privacy Policy**.

a. Personally Identifiable Information (PII)

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations require agencies to protect PII, which is any information that permits the identity of an individual to be directly or indirectly inferred. This includes information linked or linkable to that individual, regardless of whether or not the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Agency.

Examples of PII, defined in **ADS 508** as "information in an identifiable form," include name, address, social security number (SSN), or other identifying number or code, telephone number, and e-mail address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals.

Additional PII-related policies appear in the following sections of this chapter:

- Section 545.2.2 Additional Roles
- Section 545.3.3.17 Privacy and Data Security
- Section 545.3.3.20 Social Media and Social Networking
- Section 545.3.6.7 Information Sharing

The USAID Privacy Office works with Program Managers, SOs, and information systems security staff to integrate sound privacy practices and controls into Agency operations. The USAID Privacy Office implements three types of documents for managing privacy practices and controls for information systems as follows:

- A Privacy Threshold Assessment or Analysis (PTA) provides a high-level description of an information system including the information it contains and how it is used. The PTA determines and documents whether or not a PIA and/or a System of Records Notice (SORN) is required.

- A Privacy Impact Assessment (PIA) is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared.

- A SORN describes the categories of records within a system of records and describes the routine uses of the data, as well as how individuals can gain access to records and correct errors.

To promote privacy compliance within the Agency, the CPO has published official guidance on the requirements and content for PTAs, PIAs, and SORNs in **ADS 508**.

b. Privacy Threshold Analyses/Information Collection Checklist

An Information Collection Checklist (ICC) serves as a Privacy Threshold Assessment or Analysis (PTA) at USAID. The ICC provides a high-level description of the system, including the information it contains and how it is used. ICCs are required whenever a new information system is being developed or an existing system is significantly modified. Program Managers and SOs are responsible for completing the ICC as part of the system development lifecycle process. The Privacy Officer reviews the ICC, who

determines whether a Privacy Impact Assessment (PIA) and/or SORN are required. ICC artifacts expire after three (3) years. Applicable controls include PL and RA.

The following policy statements apply to privacy threshold analyses/information collection checklist:

(1) An ICC must be conducted as part of new information system development or whenever an existing system is significantly modified. ICC artifacts expire after three (3) years, and a new ICC must be submitted.

(2) An ICC must be conducted whenever an information system undergoes a security authorization.

(3) The USAID CPO must evaluate ICC's to determine if the respective system contains PII elements or privacy information and if the system requires a PIA and a SORN.

(4) Information systems must not be designated operational until the USAID Privacy Office approves the ICC.

(5) For Privacy Sensitive Systems, the confidentiality security objective must be assigned an impact level of moderate or higher.

c. Privacy Impact Assessments (PIA)

PIA statements are representative documents of the processes used to determine if USAID's information handling practices conform to established legal, regulatory, and policy frameworks for privacy protection. Information handling practices include both manual processes, as well as USAID automated technology processes. Applicable control includes PL.

The following policy statements apply to PIA:

(1) PIAs are required (as determined by the PTA) as part of new information system development or whenever an existing system is significantly modified.

(2) Information systems which the USAID Privacy Office has determined require a PIA must not be designated operational until the USAID Privacy Office approves the PIA for that system.

d. System of Records Notices (SORN)

The Privacy Act of 1974 requires a SORN when PII is maintained by a Federal agency in a system of records and the PII is retrieved by a personal identifier. A system of records is "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual," according to the Privacy Act.

The term "system of records" is not synonymous with an information system and can include paper as well as electronic records. SORNs can cover the records in a single group of records or a single information system, or they can cover multiple groups of records or multiple information systems.

Information systems considered a system of records may not be designated operational until a SORN has been published in the Federal Register for thirty (30) days. OMB, specifically Privacy Act Implementation, Guidelines and Responsibilities, July 9, 1975, and **OMB A-130**, including Appendix I, are the benchmark references for SORNs.

OMB requires each SORN to be reviewed every two (2) years to ensure that it accurately describes the system of records. This process is the Biennial SORN Review Process. The USAID Privacy Office works with SOs to ensure that SORN reviews are conducted every two (2) years following publication in the Federal Register. Applicable control includes CA.

The following policy statements apply to SORNs:

(1) A SORN is required when PII is maintained by a Federal agency in a system of records where information about an individual is retrieved by a unique personal identifier.

(2) Information systems containing PII must not be designated operational until a SORN has been published in the Federal Register for thirty (30) days.

(3) SOs must review and republish SORNs every two (2) years as required by **OMB A-130**.

e. Protecting Privacy Sensitive Systems

OMB M-06-16, Protection of Sensitive Agency Information, requires agencies to protect PII that is physically removed from Agency locations or is accessed remotely. Physical removal includes both removable media as well as media within mobile devices (i.e., laptop hard drive). Applicable controls include MP and SC.

The following policy statements apply to protecting privacy sensitive systems:

(1) PII removed from USAID facilities on removable media, such as CDs, DVDs, laptops, and Personal Digital Assistants (PDAs), must be encrypted, unless the information is being sent to the individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.

(2) If PII can be physically removed from an information system (e.g., printouts, CDs),the SSP must document the specific procedures, training, and accountability measures in place to ensure that remote use of the data does not bypass the protections provided by the encryption.

(3) Systems which, as part of routine business, remove PII in the form of a Computer-Readable Extract (CRE), e.g., routine system-to-system transmissions, must address associated risks in the SSP.

(4) PII contained within a non-routine or ad hoc CRE (e.g., CREs not included within the boundaries of a source system's SSP) must not be removed, physically or otherwise, from a USAID facility without written authorization from the Data Owner responsible for ensuring that the disclosure of the CRE data is lawful and in compliance with this and applicable USAID privacy and security policies.

(5) All ad hoc CREs must be documented, tracked, and validated every ninety (90) days after their creation to ensure that their continued authorized use is still required or that they have been appropriately destroyed or erased.

(6) Ad hoc CREs must be destroyed or erased within ninety (90) days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data must be documented by the Data Owner and audited periodically by the USAID Privacy Officer.

f. Privacy Incident Reporting

The USAID Privacy Office is responsible for implementing the Agency's privacy incident response program based on requirements in **OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information**, May 22, 2007. Through close collaboration, the USAID CPO, CIO, and CISO must ensure that all USAID privacy and computer security incidents are identified, reported, and appropriately responded to. The purpose is to mitigate harm to USAID assets, information, and staff. Incidents involving PII are subject to strict reporting standards and timelines. Applicable control includes IR.

The following policy statements apply to privacy incident reporting:

(1) Any SO discovering a suspected or confirmed privacy incident must coordinate with the Privacy Officer and CISO to evaluate and subsequently report the incident to the United States Computer Emergency Readiness Team (US-CERT) within one (1) hour of discovery.

(2) The Privacy Officer, in cooperation with the CISO, must jointly evaluate the incident, but the CISO is responsible for reporting the incident to US-CERT.

(3) USAID staff must also report suspected or confirmed privacy incidents or incidents involving PII to their supervisor or the USAID CIO-Helpdesk immediately upon discovery/detection, regardless of the manner in which the incidents might have occurred.

(4) SOs must follow the **USAID Incident Handling Guide**. [For a copy of this document, please contact the Information Assurance Division at **isso@usaid.gov**.]

545.3.3.18 E-Authentication

Effective Date: 11/09/2012

Identity verification or authentication, known as e-authentication, secures online Government services and protects individual privacy.

To determine if e-authentication requirements apply, each system must have an evaluation. Only federated identity providers approved through the Federal CIO Council's Identity, Credentialing, and Access Management's (ICAM) Trust Framework Provider Adoption Process (TFPAP) can make the determination. For more information on the Federal Identity, Credentialing, and Access Management (FICAM) initiative, please see **Idmanagement.gov**. Applicable controls include IA and PL.

E-authentication guidance appears in the following documents:

- **OMB M-04-04, E-Authentication Guidance for Federal Agencies**
- **NIST SP 800-63, Electronic Authentication Guideline**

The following policy statements apply to e-authentication:

(1) For systems that allow online transactions, the SO must determine whether e-authentication requirements apply.

(2) SOs must determine the appropriate assurance level for e-authentication by following the steps described in **OMB M-04-04, E-Authentication Guidance for Federal Agencies**.

(3) SOs must implement the technical requirements described in **NIST SP 800-63, Electronic Authentication Guideline**, at the appropriate assurance level for those systems with e-authentication requirements.

(4) SOs must ensure that each SSP reflects the e-authentication status of the respective system.

(5) Programs considering the use of e-authentication must conduct a PTA to view of privacy risks and how they will be mitigated.

(6) Existing physical and logical access control systems must be upgraded to use Personal Identity Verification (PIV) credentials, in accordance with NIST and USAID guidelines.

(7) All new systems under development must be enabled to use PIV credentials, in accordance with NIST and USAID guidelines, prior to being made operational.

545.3.3.19 CFO Designated Systems

Effective Date: 11/09/2012

USAID CFO Designated Systems require additional management accountability to ensure effective internal control exists over financial reporting. The USAID CFO maintains the approved list of CFO Designated Systems. Refer to the CFO Page for more information.

This section provides additional system requirements based on **OMB Circular A-123, Management's Responsibility for Internal Controls, Appendix A**. Requirements in this circular have been mapped to **NIST SP 800-53, Rev. 3** controls. These requirements are in addition to other security requirements established in this document and other CFO-developed financial system requirements. Where a conflict exists between this section of ADS 545 and other statements of requirements for CFO Designated Systems, this section takes precedence.

Requirements strengthen the assessment process designed to assure internal control over financial reporting. The strengthened process requires management to document

the design and test the operating effectiveness of controls for CFO Designated Systems. The SO is responsible for ensuring that all requirements, including security requirements, are implemented in USAID systems. The CISO must coordinate with the CFO organization to ensure that these requirements are met. Applicable controls include CA, RA, CP, IR, CM and PL.

Note that the **ADS 596, Management Accountability and Controls** contains additional information on the subject.

The following policy statements apply to CFO designated systems:

(1) SOs are responsible for annual security assessments of key security controls for CFO Designated Systems in CSAM or other CISO-approved automated security assessment tools.

(2) The CFO must identify, publish and review the systems which must comply with additional internal controls, and the CFO must review and publish a list of such Agency financial systems annually.

(3) The CISO must conduct vulnerability assessments and verification of critical patch installations on all CFO Designated Systems.

(4) All CFO Designated Systems must have a minimum impact level of “moderate” for confidentiality, integrity, and availability. If warranted by a risk-based assessment, the integrity objective must be “high.”

(5) The CFO must approve and sign all security accreditations for CFO Designated Systems.

(6) SOs must create CPs for all CFO Designated Systems requiring moderate availability and DRPs for all CFO Designated Systems requiring high availability and then test each plan annually.

(7) The CISO must ensure routine incident response tracking for all CFO Designated Systems.

(8) The CISO must report incidents related to CFO Designated Systems to the CFO.

(9) An SSP update for CFO Designated Systems must occur at least annually. The SSP must identify key controls assigned by the CISO.

(10) The SO must request a waiver or exception from the CISO if a key control weakness is identified for a CFO Designated System but not remediated within twelve (12) months.

(11) The CFO must assign a dedicated ISSO to each CFO Designated System. CFO Designated System ISSOs may be assigned to more than one CFO Designated System.

(12) CFO Designated System ATOs will be rescinded if SOs fail to comply with testing and reporting requirements of this policy.

(13) The CFO coordinates with the CISO to approve any major system changes to CFO Designated Systems identified in the USAID system inventory.

545.3.3.20 Social Media and Social Networking

Effective Date: 11/09/2012

Social Media hosts are public, content-sharing Web sites which allow individual users to upload, view, and share content such as video clips, press releases, opinions and other information. Contact the USAID Bureau of Legislative and Public Affairs (LPA) for the current Terms of Service (TOS) and guidelines for posting to these sites.

In some cases the Agency develops its own and in other cases endorses those published by other Federal agencies, such as the General Services Administration (GSA) or Office of Personnel Management (OPM). Examples of social media include Internet forums, videos, wikis, blogs, virtual worlds, podcasts, and social networking sites. Social Media service may be approved on one network but not others, because different networks have different risk acceptance levels. Applicable control includes SA.

The following policy statements apply to social media and social networking:

(1) The Privacy Office must conduct a PIA on information collected.

(2) The CISO must conduct a security categorization of the information types.

(3) The CISO must conduct a risk-based assessment to determine if users can access the particular Social Media technology and if limitations are appropriate.

(4) The CISO must verify that the Agency has approved the Social Media service provider TOS agreement before authorizing staff to post information on a social media site.

(5) The CISO must maintain an inventory of approved social media sites.

(6) The CISO must provide training material to staff for the use of approved social media.

The following policy statements apply to staff assigned responsibility for operating an official account or contributing to a Social Media Web site:

Note: The site can be a USAID site or an external commercial service, functioning on behalf of the Agency.

(1) Staff using Social Media technologies in an official capacity must do so only on Agency-approved accounts and may only use official e-mail or other official contact information to create and manage those accounts.

(2) Staff must post official Agency positions only if authorized to do so.

(3) Staff must not post Sensitive but Unclassified (SBU) to include PII on a Social Media Web site unless the **Privacy Act** and **Freedom of Information Act** (FOIA) permit release of the information. For additional information on the PII release, direct questions to the CPO or the FOIA Officer.

(4) Staff must ensure that the content maintained on their Social Media sponsors' Web sites is secure and adequately safeguarded from unauthorized disclosure or destruction.

(5) The improper release of PII or other sensitive information may result in civil or criminal penalties, in accordance with the Privacy Act.

(6) The records must be retained consistent with the records retention requirements, including **NARA Bulletin 2011-02, Guidance on Managing Records in Social Media Platforms**.

(7) Only LPA-designated content managers may post content on behalf of the Agency or be granted access to the site on a continuing basis.

(8) Posted content must follow Agency TOS and guidelines, which cover social media hosts like YouTube or Twitter or any hosts endorsed by the Agency such as GSA or OPM.

(9) Content must not be posted to any social media site for which the Agency has not approved and published final posting guidelines and TOS.

(10) Content managers must review and understand the appropriate Agency-level TOS for the appropriate social media host.

(11) Content managers must make a risk decision prior to posting any information. They must recognize that social medial hosts are subject only to TOS but not to USAID policy. They must bear in mind that released information is no longer under USAID control.

For additional information, see **ADS 565, Physical Security Programs (Domestic)** and **ADS 566, Personnel Security Investigations and Clearances**.

545.3.4 Operational Policies

Effective Date: 11/09/2012

Operational policies address security that focuses on controls that are usually implemented and executed by people, as opposed to systems. These controls often require technical or specialized expertise, and often rely upon management activities as well as technical controls.

545.3.4.1 Personnel Security

Effective Date: 11/09/2012

USAID systems face threats from many sources. The intentional and unintentional actions of system users can harm or disrupt USAID systems and facilities. Such actions could destroy or modify data, deny service, disclose unauthorized data. To reduce the threat risk, stringent safeguards must be in place.

a. Citizenship, Personnel Screening, and Position Categorization

Applicable control includes PS.

The following policy statements apply to citizenship, personnel screening, and position categorization:

(1) The CISO must develop, disseminate and review/update annually personnel security policy.

(2) SOs must document procedures to implement personnel security policy and associated controls.

(3) The Agency must designate position sensitivity level for all Government and contractor positions which use, develop, operate, or maintain information systems. The COR must determine risk levels for each contractor position annually and revise them as needed.

(4) SOs must ensure favorably adjudicated background investigations of position incumbents commensurate with the defined position sensitivity levels.

(5) SOs must ensure that no Federal employee without a favorably adjudicated background investigation has access to USAID systems.

(6) SOs must ensure that no contractor without a favorably adjudicated background investigation has access to USAID systems.

For additional information, see **ADS 565** and **ADS 566**.

b. Rules of Behavior (ROB)

The ROB appears in role-based and system-based subdocuments used to support ADS Chapter 545. The ROB delineates the responsibilities and behaviors for each staff role as well as consequences of behavior not consistent with the ROB. SOs, GSS ISSO, and the CISO must establish and disseminate ROB for each of their respective information systems, so that staff is aware of the security rules that pertain to their particular job functions and roles. Applicable controls include PL and AT.

The following policy statements apply to ROB:

(1) The CISO must define and maintain ROB for roles in the USAID network.

(2) SOs must define and maintain ROB for all information systems in their charge.

(3) SOs must ensure ROB acknowledge that the user has no expectation of privacy (a “Consent to Monitor” provision) and that disciplinary actions may result from violations.

(4) The CISO must verify the content of the System ROB defined by each SO.

(5) SOs must ensure that each USAID user attends ROB training and signs a copy of the ROB prior to getting access to a system user account or data.

(6) The ROB may be combined for various systems and roles as long as SOs agree that rules are sufficient for their respective systems.

The USAID ROB combines the five user classifications derived from chapter policies. Additional ROB, as defined by SOs for each of their respective USAID information systems, must be filed with the information SSP.

c. Access to Sensitive Information

Applicable control includes AC.

The following policy statement applies to access to sensitive information:

- SO must ensure that users have a valid have a valid requirement to access systems supporting their programs.

d. Separation of Duties

Separation of duties helps prevent a single individual from disrupting or corrupting a critical security process. Applicable control includes AC.

The following policy statements apply to separation of duties:

(1) SOs must divide and separate duties and responsibilities of critical information system functions among different individuals or groups. This minimizes fraudulent or criminal activities caused by unauthorized system access.

(2) The appropriate AO must review and approve persons requiring administrator privileges. The AO may delegate this duty to an appropriate Functional or Program Manager who is a government employee.

(3) Persons requiring administrator privileges must be assigned administrator accounts separate from their user accounts as authorized by the AO and created by the SA.

(4) Persons with administrator accounts must use them only for administrator duties. Persons must use their user accounts to perform all other functions (checking e-mail and accessing the Internet) not directly tied to administrator duties.

e. Information Security Awareness, Training, and Education

Awareness, training and educational programs provide knowledge and instruction for operating information systems and data protection. Applicable control includes AT.

The following policy statements apply to information security awareness, training, and education:

(1) The CISO must establish, document, and implement, and review/update annually, a formal security awareness and training policy and program for users of USAID information systems.

(2) USAID employees, contractors, or others working on behalf of USAID accessing USAID systems must receive initial training and annual refresher training in security awareness and accepted security practices. Staff must complete security awareness within forty-eight (48) hours of being granted a user account. If the user fails to comply, user access must be suspended. When access to an Information system (IS) system is contractual the COR must ensure that contractors complete the necessary training sessions.

(3) USAID employees, staff, contractors, or others working on behalf of USAID with significant security responsibilities (e.g., ISSOs and SAs) must receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities. When access to an Information system (IS) system is contractual the COR must ensure that contractors complete the appropriate specialized training and refresher courses.

(4) The CISO must maintain training records, to include trainee name and position, type of training received, and costs of training. SO may maintain records of additional training received.

(5) User accounts and access privileges, including access to email, must be disabled for users without annual refresher training unless the CISO grants a waiver.

(6) The SO must provide evidence of training by submitting copies of training schedules, training rosters, and training reports, upon request of IG, the CISO, or other governing entities.

(7) The CISO must review information security awareness programs annually.

f. Separation From Duty

Applicable controls include AC and PS. The following policy statements apply to separation from duty:

(1) SOs must implement procedures to revoke access for USAID employees, contractors, or others working on behalf of USAID who leave the Agency, take up other duties, or no longer need access.

(2) SOs must establish procedures to recover all USAID information system-related property and assets from departing individual and transfer sensitive information stored on any media to an authorized individual.

(3) Accounts for users on extended absences must be temporarily suspended or disabled. Refer to the Agency's **Computer Security User Account Management Procedures.** [For a copy of this document, please contact the Information Assurance Division at **isso@usaid.gov**.]

(4) SOs must review information system accounts supporting their programs at least annually.

545.3.4.2 Physical and Environmental Protection

Effective Date: 11/09/2012

a. Physical and Environmental Protection

Applicable controls include PE and PM.

The following policy statements apply to physical and environmental controls:

(1) The CISO must develop, disseminate, and review/update annually a documented physical and environmental protection policy.

(2) SOs and/or responsible offices must establish, implement and enforce documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

As part of the physical and environmental policy:

(1) The Office of Security (SEC) must develop and keep current a list of staff and personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

(2) SEC must issue authorization credentials;

(3) SEC must review and approve the access list and authorization credentials within a defined frequency, removing from the access list staff no longer requiring access;

(4) SEC must secure keys, combinations, and other physical access devices;

(5) SEC must Inventory physical access devices;

(6) SEC must change combinations and keys and when keys are lost, combinations are compromised, or individuals are transferred or terminated; and

(7) SEC must control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Note: Facilities Management refers to either the designated management for the building under contract or agreement to the Agency and/or HQ Management Division (M/MS/HMD).

In collaboration with the SO or Mission Directors,

(1) Facilities Management must protect power equipment and power cabling for the information system from damage and destruction;

(2) Facilities Management must provide the capability of shutting off power to the information system or individual system components in emergency situations; place emergency shutoff switches or devices in location by information system or system component. The purpose is to facilitate safe and easy access for staff; and protect emergency power shutoff capability from unauthorized activation;

(3) Facilities Management must provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss;

(4) Facilities Management must employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility;

(5) Facilities Management must employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source;

(6) Facilities Management must maintain and monitor, acceptable temperature and humidity levels, within the facility where the information system resides;

(7) Facilities Management must protect the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key staff;

(8) Facilities Management must authorize, monitor, and control types of information system components entering and exiting the facility and must maintain records of those items;

(9) Facilities Management must employ management, operational, and technical information system security controls at alternate work sites; must assess as feasible the effectiveness of security controls at alternate work sites; and must provide a means for employees to communicate with information security staff in case of security incidents or problems;

(10) Facilities Management must position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access;

(11) Facilities Management must ensure that only authorized staff can have access to USAID buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data;

(12) Facilities Management must ensure controls for deterring, detecting, restricting, and regulating access to sensitive areas must be in place and must be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters;

(13) Facilities Management must ensure controls are based on the level of classification and risk, determined in accordance with Agency security policy as reflected in this and other relevant documents; and

(14) Facilities Management must ensure visitors sign in upon entering USAID facilities which house information systems, equipment, and data; must

ensure visitors are escorted during their stay; and must ensure that visitors sign out upon leaving. Non-USAID contractor or vendor access must be limited to those work areas requiring their presence. Visitor logs must be maintained and available for review for one (1) year.

For more information refer to **ADS 562** and **ADS 565.**

b. Sensitive Facility

Facilities processing, transmitting, or storing sensitive information must incorporate physical protection measures based on the level of risk. Agency security policy in this and other relevant documents must be part of risk determination. Applicable controls include PE and PM.

545.3.4.3 Media Controls

Effective Date: 11/09/2012

a. Media Protection

All staff must store media, when not in use, with sensitive information like hard copy media, backup media, and removable media such as USB drives, in secure locations. These include a locked office, room, desk, file cabinet, locked tape device, or other storage prohibiting access by unauthorized person. Applicable controls include MP, PE, CP, IA, PM, SI, AC, and SC.

The following policy statements apply to media protection:

(1) The CISO must develop, disseminate and review/update annually a documented media protection policy.

(2) SOs must document and enforce procedures to implement media protection policies and associated media protection controls.

(3) Only USAID-issued removable media, to include Universal Serial Bus (USB) drives, are authorized for use to store Agency information or connect to Agency equipment.

(4) Systems requiring encryption must comply with Section 545.3.5.5, Cryptography, subsection a. Encryption. USAID-owned USB drives must use Agency-approved encryption.

(5) USAID-owned USB and other removable media must use Agency-approved encryption.

(6) Staff must follow established procedures to protect paper and electronic outputs from systems which hold sensitive information.

(7) Staff must protect printed output. Printing of sensitive documents must occur only when a trusted person attends the printer.

(8) Staff must follow the procedures established by **Media Handling Procedures and Guidelines** for the transportation or mailing of sensitive media.

b. Media Marking and Transport

Applicable control includes MP.

The following policy statements apply to media marking and transport:

(1) Media known by the information owner to contain sensitive information must be appropriately marked in accordance with **Media Handling Procedures and Guidelines**.

(2) SOs and staff must control the transport of information system media containing sensitive data, outside of controlled areas and restrict pickup, receipt, transfer, and delivery to authorized staff.

c. Media Sanitization and Disposal

Applicable control includes MP.

The following policy statements apply to media sanitization and disposal:

(1) SOs and staff must use CISO-approved methods to sanitize any information system storage medium that has sensitive information, before disposal, reuse, recycle, or return to the owner or manufacturer.

(2) SOs must maintain records of the sanitization and disposition of information systems storage media.

(3) SOs must periodically test USAID degaussing equipment to verify the equipment works.

d. Production, Input/Output Controls

Applicable control includes SI.

The following policy statements apply to production, input/output controls:

(1) SOs must follow established procedures to significantly reduce the risk of access or theft of sensitive information by unauthorized individuals.

(2) These procedures must address not only the system hardcopy and electronic outputs, but also the transportation or mailing of sensitive media.

545.3.4.4 Video and Voice Communications Security

Effective Date: 11/09/2012

Voice and video communications consist of information shared orally or visually such as telephone and videoconferencing. Applicable controls include CM and PL.

The following policy statements apply to video and voice communications security:

(1) Users must use only Agency approved video and voice communication systems to transmit, process, and store SBU information.

(2) Classified national security information must not, under any circumstances, be discussed over unsecured telephones.

(3) Users must not process, store, transmit, or receive classified information on any system, to include Video and/or voice systems, unless those systems are specifically designated for classified information. For additional information on classified systems and information, see **ROB for Users**.

(4) SOs must categorize their systems as moderate or high in order to process, store, transmit, or receive SBU to include PII.

(5) SOs must ensure that their voice and/or video systems comply with federal mandates and Agency policy, except where the CISO provides a waiver.

a. Video Teleconferencing

Applicable controls include AC, PE, and SC.

The following policy statements apply to video teleconferencing:

(1) SOs must implement controls to ensure that only authorized individuals participate in each videoconference.

(2) SOs must ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.

(3) Video teleconferencing equipment and software must be disabled or powered off when not in use.

b. Voice Over Data Networks

Voice over Internet Protocol (VoIP) and similar technologies move voice over digital networks. These technologies use protocols originally designed for data networking. Such technologies include Voice over Frame Relay, Voice over Asynchronous Transfer Mode, and Voice over Digital Subscriber Line. Applicable controls include SC and PM.

The following policy statements apply to voice over data networks:

(1) Prior to implementing voice over data network technology, SOs must coordinate with CISO to conduct rigorous risk assessments and security testing and provide a business justification for their use. Any systems that employ this technology must be accredited for this purpose with residual risks clearly identified.

(2) Voice over data network implementations must have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.

(3) SOs must implement appropriate identification and authentication controls, audit logging, and integrity controls on every element of their voice over data networks.

(4) SOs must restrict physical access to voice over data network elements to authorized staff.

545.3.4.5 Data Communications

Effective Date: 11/09/2012

a. Telecommunications Protection Techniques

Applicable control includes CM.

The following policy statements apply to telecommunications protection techniques:

(1) SOs must select the telecommunications protection techniques that meet information security needs, in the most cost-effective manner, consistent with Agency information system security policies.

(2) CISO-approved protected network services may be used as cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.

b. Facsimiles

Applicable controls include SC and AC.

The following policy statements apply to facsimiles:

(1) SOs must implement and enforce technical controls on fax technology and systems (including fax machines, servers, gateways, software, and protocols) which transmit and receive sensitive information.

(2) SOs must configure fax servers so they do not enable incoming lines to access the network or any data on the fax server.

545.3.4.6 Wireless Communications

Effective Date: 11/09/2012

Wireless telecommunications is the transfer of information between two (2) or more points not physically connected. Distances can be short, such as a few feet, or as far as a thousand miles. There are many security risks inherent to wireless communications. Information security on wireless communications must include special precautions. Applicable controls include AC, IA, and SC.

Wireless network communications technologies include the following:

- Wireless systems (e.g., wireless local area networks [WLAN], wireless wide area networks [WWAN], wireless personal area networks [WPAN], peer-to-peer wireless networks, and information systems which leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols;

- Wireless mobile electronic devices (MCDs), described in section b below;

- Wireless tactical systems, including mission-critical communication systems and devices (e.g., Land Mobile Radio [LMR] subscriber devices and infrastructure equipment, remote sensors, and technical investigative communications systems); and

- Radio Frequency Identification (RFID).

For additional information, see **Wireless Access Standards and Guidelines.**

The following policy statements apply to wireless network communications:

(1) Only CISO-approved Wireless network communications and applications technologies are authorized for use within USAID.

(2) If used, Public Key Infrastructure (PKI)-based encryption on wireless systems, wireless MCDs, and wireless tactical systems must implement and maintain a key management plan approved by the CISO.

a. Wireless Systems

Applicable controls include CA, PM, AC, SC, and SI.

The following policy statements apply to wireless systems:

(1) Annual information security assessments must be conducted on all approved wireless systems. Wireless information security assessments must detail vulnerabilities, risk statements, risk levels, and corrective actions.

(2) A POA&M must be developed to address wireless information security vulnerabilities.

(3) SOs must coordinate with the CISO to identify countermeasures to denial-of-service attacks and to complete a risk-based evaluation prior to approving the use of a wireless MCD.

(4) SSPs and system design must include a strategy that integrates firewalls, screening routers, wireless intrusion detection systems, antivirus software, FIPS 140-2 validated encryption, strong authentication, and cryptographic key management (when required).

(5) SOs must document all wireless usage and include such use in their system SSP.

(6) The CISO must establish usage restrictions and implementation guidance for wireless technologies and authorize, monitor, and control wireless access to USAID information systems.

b. Wireless Mobile Computing Devices (MCDs)

Wireless MCDs include PDAs, smart telephones, two-way pagers, handheld radios, cellular telephones, PCS devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices, and any other wireless devices capable of storing, processing, or transmitting sensitive information. Applicable controls include AC, CA, CM, PL, IA, SC, SI, PE, MP, and PM.

For additional information, see **Mobile Computing Standards and Guidelines**.

The following policy statements apply to wireless MCDs:

(1) Wireless MCDs and accessory devices must not be used in areas where classified information is discussed, maintained, or distributed, unless specifically authorized by the CISO in writing.

(2) Wireless MCDs must not be used to store, process, or transmit combinations, PINs, or sensitive information in unencrypted formats.

(3) Wireless MCDs such as BlackBerry devices and smart phones must implement strong authentication, data encryption, and transmission encryption technologies. Portable electronic devices such as BlackBerry devices and smart phones must be password-protected, with a security timeout period established.

(4) SSPs must detail the provisions, procedures, and restrictions for using wireless MCDs to download mobile code in an approved manner.

(5) Wireless MCDs must be operated only when current USAID approved versions of antivirus software and software patches are installed.

(6) Cost-effective countermeasures to Denial-of-Service (DOS) attacks must be identified and established prior to a wireless MCD approval.

(7) SOs must maintain a current inventory of all approved wireless MCDs in operation.

(8) Wireless MCDs must be cleared of all information before reuse by another individual, office, or Bureau within USAID or before they are surplused; wireless MCDs that are being disposed of, recycled, or returned to the owner or manufacturer must first be sanitized using approved procedures.

(9) Legacy wireless MCDs not compliant with USAID information security policy must undergo a migration plan. This must describe the provisions, procedures, and restrictions for transitioning these wireless MCDs to USAID-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the CISO.

(10) The CISO and SO approve the use of Government-owned MCDs to process, store, or transmit sensitive information.

Please refer to **ADS 552, Classified Information Systems Security**.

c. Cellular Phones

Applicable control includes PL.

The following policy statements apply to wireless cellular phones:

(1) SOs must develop CISO-guidance for discussing sensitive information on cellular phones.

(2) Under no circumstances must classified information be discussed on cellular phones.

d. Pagers

Applicable control includes PL.

The following policy statement applies to pagers:

- Pagers must not be used to transmit sensitive information.

e. Multifunctional Wireless Devices

Wireless devices like cell phones, pagers, and radios which can surf the Internet, retrieve email, and take and transmit pictures) are multifunctional. Most of these functions do not have sufficient security. Applicable controls include AC, SC and PE.

The following policy statements apply to multifunctional wireless devices:

(1) Devices that cannot be encrypted using approved cryptographic modules must not be used to process, store, or transmit sensitive information.

(2) Short Message Service (SMS) and Multimedia Messaging Service (MMS) must not be used to process, store, or transmit sensitive information, and should be disabled whenever possible.

f. Wireless Tactical Systems

In some limited circumstances such as Missions supported by the Office of Foreign Disaster Assistance (OFDA), Wireless Tactical Systems may be required for use. Wireless tactical systems include Land Mobile Radio subscriber devices, infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed under circumstances in which staff safety and Mission success are at stake, wireless tactical systems require even greater security measures. Applicable controls include CM, IA, SC, and PM.

The following policy statements apply to wireless tactical systems:

(1) SOs must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system.

(2) Wireless Tactical Systems must be approved by the USAID CISO before use.

545.3.4.7 Overseas Communications

Effective Date: 11/09/2012

Where required or appropriate, all communications outside of the United States and its territories must be in accordance with the Department of State Foreign Affairs Manual (FAM), **12 FAM 600, Information Security Technology.**

545.3.4.8 System Maintenance

Effective Date: 11/09/2012

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. Applicable control includes MA.

The following policy statements apply to system maintenance:

(1) The CISO must develop, disseminate, and review/update annually a documented maintenance policy.

(2) SOs must document and enforce procedures to implement the maintenance policy and associated maintenance security controls.

(3) SOs must schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

(4) SOs must control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

(5) SOs must require that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

(6) SOs must sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.

(7) SOs must check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

(8) SOs must approve, control, monitor the use of, and maintain on an ongoing basis, information system maintenance tools.

(9) SOs must not allow non-local maintenance and diagnostic activities. SOs must establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel.

(10) SOs must ensure that personnel performing maintenance on the information system have required access authorizations or designate organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

(11) SOs must obtain maintenance support and/or spare parts for security-critical information system components and/or key information technology components within a defined time period of failure.

545.3.4.9 Equipment

Effective Date: 11/09/2012

a. Workstations

Applicable controls include AC, CM, and PE.

The following policy statements apply to workstations:

(1) SOs must configure workstations to either log off, or activate a password-protected lock or a password-protected screensaver within fifteen (15) minutes of user inactivity.

(2) SOs must protect workstations and laptops from theft.

(3) Staff must either log off or lock their workstations when unattended.

b. Laptop Computers and Other MCDs

The following policy statements apply to laptop computers and other MCDs:

(1) SOs must configure workstations to either log off, or activate a password-protected lock or a password-protected screensaver within fifteen (15) minutes of user inactivity.

(2) SOs and Staff must protect laptops and other MCDs from theft.

(3) Staff must either log off or lock their workstations when unattended.

(4) Information stored on any laptop computer or other MCD that may be used in a residence or on travel must use encryption in accordance with Section 545.3.5.5(a) Cryptography (Encryption), for data at rest and in motion.

(5) Passwords, hardware-based tokens, and Smart Cards must not be stored on or with the laptop or other MCD.

(6) Laptop computers and other MCDs when unattended in offices must be secured via a locking cable, locked office, or locked cabinet or desk.

c. Personally Owned Equipment and Software

Applicable controls include SA and AC.

The following policy statements apply to personally owned equipment and software:

(1) Personally owned equipment and software must not be used to store sensitive information.

(2) Equipment not owned or leased by the Federal Government or operated by a contractor on behalf of the Federal Government must not be physically connected to USAID equipment or networks without the written prior approval of the CISO.

(3) Personally owned software must not be installed on Government equipment unless specifically authorized in writing by the Office of the CIO (OCIO) Change Control Board (CCB) and the CISO.

d. Hardware and Software

Applicable controls include CM, AC, RA, MA, and SI.

The following policy statements apply to hardware and software:

(1) SOs must ensure that information systems follow the hardening guides for operating systems and the configuration guides for applications.

(2) SOs must limit system software and hardware access to authorized personnel.

(3) SOs must test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their CMP.

(4) SOs must manage systems to reduce vulnerabilities through vulnerability testing and management, prompt patch installation, and elimination or disabling of unnecessary services.

(5) SOs must, if applicable, disable maintenance ports during normal system operation and enable them during approved maintenance activities.

(6) SOs must employ tools and/or processes known as integrity mechanisms to detect unauthorized changes to software and information. These

mechanisms, facilitated by developing secure software, which use engineering best practices, could include parity checks, cyclical redundancy checks, cryptographic hashes, and more.

(7) Only cleared staff with technical knowledge sufficient to detect and prevent unauthorized modification to information systems or networks are authorized to monitor and escort the maintenance personnel during maintenance activities.

(8) Maintenance using a different user's identity may be performed only when the user is present. User must log in and observe the maintenance actions at all times. User must not share authentication information with maintenance personnel.

e. Personal Use of Government Office Equipment and USAID Systems/ Computers

Applicable controls include AC and PL.

The following policy statements apply to personal use of government office equipment and USAID systems/computers:

(1) USAID employees, contractors or persons working on behalf of USAID may use Government office equipment and USAID information systems for authorized purposes only. "Authorized use" includes limited personal use as described in USAID acceptable use policy documents, for example, **Internet Acceptable Usage Policy** and **E-Mail Acceptable Usage Policy.**

(2) Limited personal use of USAID e-mail and Internet services must not interfere with official duties, inhibit the security of information and information systems, or cause degradation of network services. Specifically prohibited activities, unless approved by the OCIO, include but are not limited to, streaming of audio or video; peer-to-peer networking and software; software or music sharing/piracy; online gaming visiting; gambling sites; hacking; and the viewing of pornography or other offensive content.

(3) Anyone granted user account access to any USAID information system must not have expectations of privacy associated with its use. By completing the authentication process, the user acknowledges his or her consent to monitoring.

(4) The use of Government office equipment and USAID information systems constitutes consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes monitoring of data transmitted outside of the network and auditing of stored data on local and network storage devices as well as removable media.

(5) All staff must sign the **ROB for Users** prior to system accounts or access to USAID systems or data. The ROB must contain a "Consent to Monitor" statement and an acknowledgement that the user has no expectation of privacy.

545.3.4.10 Agency Information Security Operations

Effective Date: 11/09/2012

The CISO is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Agency. Applicable controls include AC, PL, IR, SI, and SC.

The following policy statements apply to Agency information security operations:

(1) USAID CIO Security Operations must lead the coordination and administration of the Agency's policy enforcement points, such as firewalls.

(2) The CIO must implement the Agency logging strategy to enable endpoint visibility and Agency situational awareness.

(3) The CISO must have the capability to process SECRET level information continuously and receive TOP SECRET (TS) and SENSITIVE COMPARTMENTALIZED INFORMATION (SCI).

(4) SEC must ensure that personnel hold appropriate clearance to access the Joint Worldwide Intelligence Communications System (JWICS). Functional and Executive managers are free to determine the number and type of personnel to be cleared, but at least two cleared persons must be available. A government employee must be available continuously for incident response and management.

(5) The CISO must establish and maintain a forensic capability and applicable procedures and guidance.

(6) The CIO must provide a vulnerability management capability, and the CISO must provide Information Security Vulnerability Management (ISVM) messages and vulnerability assessment capabilities.

(7) The CISO must apprise the CIO of all pertinent matters involving the security of information systems and distribute that security-related decisions and information to the ISSOs and other appropriate persons.

545.3.4.11 Incident Management and Response

Effective Date: 11/09/2012

Incident Management and Response is an important component of information technology (IT) programs. Security-related threats are not only more numerous and diverse but also more damaging and disruptive. An incident response capability is therefore necessary for quickly detecting incidents, minimizing loss and destruction, mitigating the exploited weaknesses, and restoring computing services. Applicable control includes IR.

a. Continuous Incident Response Capability

The following policy statements apply to continuous incident response capability:

(1) The CISO must establish, disseminate and review/update annually, a documented incident response policy and procedures to facilitate the implementation of the policy.

(2) SOs must coordinate with the CISO to implement and enforce incident response policy and associated incident response controls.

(3) The Agency must establish and maintain a Continuous Incident Response Capability.

(4) As part of the Continuous Incident Response Capability, the CISO must:

- Train staff in their incident response roles and responsibilities with respect to the information system; and Provide refresher training annually; and
- Test and/or exercise the incident response capability for the information system using tests and/or exercises to determine the incident response effectiveness and documents the results.

(5) Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; coordinate incident handling activities with contingency

planning activities; and incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises; and implement the resulting changes accordingly; activities include the following:

- Track and document information system security incidents;
- Require staff to report suspected security incidents to the organizational incident response capability within defined time periods and report security incident information to designated authorities;
- Provide an incident response support resource, integral to the Agency incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents;
- Develop an incident response plan that provides the Agency with a roadmap for implementing its incident response capability;
- Describe the structure and organization of the incident response capability;
- Provide a high-level approach for how the incident response capability fits into the overall organization;
- Meet the unique requirements of the organization, which relate to mission, size, structure, and function;
- Define reportable incidents;
- Provide metrics for measuring the incident response capability within the organization;
- Define the resources and management support needed to effectively maintain and mature an incident response capability, and to include a review and approval by designated officials within the organization;
- Distribute copies of the incident response plan to the defined list of incident response staff (identified by name and/or by role) and organizational elements;
- Review the incident response plan annually;

- Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and

- Communicate incident response plan changes to a defined list of incident response staff (identified by name and/or by role) and organizational elements.

b. User Support

The following policy statements apply to user support capability:

(1) The Agency must establish and facilitate a user support capability to generate an initial response and react to a reported security incident;

(2) The Agency must establish and maintain 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.);

(3) The Help Desk, SAs, 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;

(4) The Help Desk or SAs must document all reported security incidents, as specified in the USAID basic or system-specific incident reporting procedures; and

(5) SOs and ISSOs must document information system-specific help desk and incident handling procedures in their information systems' System Security Plans.

More information on USAID Continuous Incident Response Capability procedures can be found in the **Incident Response Program Guide.** [For a copy of this document, please contact the Information Assurance Division at **isso@usaid.gov**.]

545.3.4.12 Documentation

Effective Date: 11/09/2012

SOs must appropriately document information systems and network so that readers understand system operation and configuration. Applicable controls include CM and SA.

The following policy statements apply to documentation:

(1) SOs must update system documentation annually or whenever system changes occur. Such changes include but are not limited to:

- Weaknesses or deficiencies discovered in currently deployed security controls after an information system breach;
- A redefinition of mission priorities or business objectives resulting in a change to the security category of the information system; and
- A change in the information system (e.g., adding new hardware, software, or firmware; establishing new connections) or the system's environment of operation;

(2) Documentation must be kept on hand and be accessible to authorized staff (including auditors) at all times.

(3) System documentation may be categorized as Sensitive if deemed appropriate by the CISO. This category will not be used as a means to restrict access to auditors or other authorized personnel.

545.3.4.13 Converging Technologies

Effective Date: 11/09/2012

Technology advances have made available devices with multiple functions. Many devices such as multifunctional desktop computers, copiers, facsimile machines, and even heating, ventilation, and air conditioning (HVAC) systems may contain sensitive data and connect to data communications networks. Applicable controls include CM, MA, MP, PE, and AC.

The following policy statements apply to converging technologies:

(1) SOs must update network printers and facsimile machines to the latest version of their firmware/software at least annually.

(2) SOs must configure network printers, copiers, and facsimile machines for at least required functionality (activating or making only those functions available necessary to achieve or support a business need).

(3) SOs must ensure that each network printer, copier, and facsimile machine is within the system definition of a USAID information system that has a current ATO.

(4) SOs must ensure that remote maintenance of network printers, copiers, and facsimile machines is conducted only from within USAID networks. If maintenance planning does not include performing remote maintenance, SOs must disable remote maintenance capabilities.

(5) SOs must configure network printers, copiers, and facsimile machines to restrict administrator access to authorized individuals or groups.

(6) SOs must ensure that maintenance or disposal of network printers, copiers, or facsimile machines, approved for sensitive reproduction, is performed only in the presence of a properly cleared person who knows how to detect inappropriate action.

(7) SOs must ensure that memory and hard drives do not leave the facility, that they are to be replaced and the old part destroyed as sensitive media.

(8) SOs must locate network printers, copiers, and facsimile machines approved to process sensitive information in areas of controlled access when the devices create paper output.

(9) Any multi-functioning device connected to a USAID network or other information system containing sensitive data must have the inbound dial-in capabilities disabled.

545.3.5 Technical Policies
Effective Date: 11/09/2012

The design of information systems which process, store, or transmit sensitive information must include the automated security features discussed in this section. Security safeguards must be in place to ensure that each person having access to sensitive information systems is individually accountable for his or her actions while utilizing the system.

545.3.5.1 Identification and Authentication
Effective Date: 11/09/2012

SOs must control and limit staff access to positive user identification and authentication mechanisms that support at least access control, least privilege, and system integrity. Applicable control includes IA.

The following policy statements apply to identification and authentication:

(1) The CISO must develop, disseminate and review/update annually a documented identification and authentication policy.

(2) SOs must document, implement and enforce procedures to comply with identification and authentication policy and associated identification and authentication controls.

(3) For information systems requiring authentication controls, SOs must configure the information system to authenticate each user before access.

(4) SOs must disable user identifiers after ninety (90) days of inactivity.

(5) USAID users must not share identification or authentication materials of any kind, or allow any other person to operate any USAID systems by employing the user's identity.

(6) All user authentication materials must be Sensitive and must carry a classification as high as the most sensitive data to which that user is granted access using that authenticator.

(7) SOs must implement strong authentication on servers, for system administrators and staff with significant security responsibilities, within one (1) year of the Agency's implementation of **Homeland Security Presidential Directive 12 (HSPD-12)** .

a. Passwords

The most common method for authenticating users is a password system that authenticates at each password use. Risk assessment must justify use of sophisticated authentication techniques, such as Smart Cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition). Applicable control includes IA.

The following policy statements apply to passwords:

(1) In password systems, the SO and/or ISSO must determine and enforce strong passwords.

(2) The ISSO must enforce how often to change passwords using guidance documentation. Without guidance, the ISSO makes sure password change occurs every ninety (90) days.

(3) USAID staff must not share personal passwords.

(4) Use of group passwords is limited to situations dictated by operational necessity or mission accomplishment. The AO and CISO must approve use of a group User ID and password.

(5) SOs must prevent embedding passwords in scripts or source code.

(6) SOs must ensure that all passwords are stored in encrypted form.

b. Biometrics

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 require careful management. Applicable control includes IA.

The following policy statements apply to biometrics:

(1) The CISO must approve all biometric authentication methods.

(2) When biometric authentication methods are in use, authentication procedures must be developed and implemented.

(3) Staff must receive training in the secure use of biometric devices.

545.3.5.2 Access Control

Effective Date: 11/09/2012

Access control limits who can interact with a resource. The resource can be a building, group of buildings, rooms, or computer-based information systems. Proper access controls ensure only authorized staff gain access to resources. Applicable controls include AC and IA.

The following policy statements apply to access control:

(1) The CISO must develop, disseminate, and review/update annually a documented access control policy.

(2) SOs must document and implement access control policy and procedures to protect resources from unauthorized alteration, loss, unavailability, or disclosure.

(3) Access control must follow the principles of least privilege and separation of duties and must require users to use unique identifiers. SSNs must not be used as login IDs.

(4) Staff must not provide their passwords to anyone, including SAs.

(5) Emergency and temporary authorization must be under strict CISO or CISO- designee control.

(6) SOs must ensure users receive unique account identifiers.

(7) USAID systems with a FIPS 199 confidentiality categorization of High must limit user concurrent sessions to one (1).

a. Automatic Account Lockout

Applicable control includes AC.

The following policy statements apply to automatic account lockout:

(1) SOs must configure each information system to automatically lock a user's account following three (3) consecutive failed logon attempts.

(2) SOs must configure accounts to automatically lock a user's account after three consecutive failed logon attempts during a twenty-four (24) hour time period.

(3) The automatic lockout period for accounts locked due to failed login attempts must be twenty (20) minutes.

(4) SOs must establish a process for manually unlocking accounts prior to the expiration of the twenty (20) minute period, after sufficient user identification. This may be done through the Help Desk.

(5) Record and periodically review all failed logon attempts in an audit log.

b. Automatic Session Termination

A session refers to a connection between a terminal device (workstation, laptop, MCD) and a networked application or system. This does not include a direct connection to a USAID network. A session also refers to access to an application or system through the USAID network, such as a database or networked application. A user may resume

activity with a locked session by re-authenticating. Terminating a session disconnects a user without saving work. Applicable controls include AC and SC.

The following policy statements apply to automatic session termination:

(1) SOs must configure networked applications or systems to automatically lock any user session in accordance with the appropriate CIO-approved configuration guide. Without guidance, the session must lock following twenty (20) minutes of inactivity.

(2) Locked sessions must remain locked until the user re-authenticates.

(3) Sessions must automatically terminate after sixty (60) minutes of inactivity.

c. Warning Banner

A warning banner alerts users they are accessing Government computers. Applicable control includes AC.

The following policy statements apply to a warning banner:

(1) All USAID systems must display a warning banner at logon.

(2) Systems internal to the USAID network must display a warning banner stipulated by the CISO.

(3) Systems accessible to the public must provide both a security and privacy statement at every entry point.

USAID system warning banners must contain at least the following statement.

> *You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.*
>
> *Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.*
>
> *By using this information system, you understand and consent to the following:*

- *You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system.*

- *Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.*

- *Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except USAID CIO.*

Note: SOs can add to this statement information that is approved by the CISO and the USAID General Counsel.

545.3.5.3 Auditing and Accountability

Effective Date: 11/09/2012

Audit records must be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records must be reviewed as specified in the SSP. Applicable controls include AU02 and PM.

The following policy statements apply to auditing and accountability:

(1) The CISO must establish, disseminate and review/update annually a documented audit and accountability policy.

(2) SOs must document, implement and enforce procedures to comply with audit and accountability policy and associated audit and accountability controls.

(3) Logs must be created whenever any of the following activities are requested to be performed by the system:

- Create, read, update, or delete confidential information, including confidential authentication information such as passwords;

- Create, update, or delete information not covered in the activity listed above;

- Initiate a network connection;
- Accept a network connection;
- User authentication and authorization for activities covered in first two activities in this list such as user login and logout;
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
- Application process startup, shutdown, or restart;
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

(4) Audit records for Agency information systems must be reviewed at least monthly. Unusual activity or unexplained access attempts must be reported to the SO and CISO.

(5) SOs must protect their audit records and logs from unauthorized change, access, or destruction.

(6) SOs must record and retain audit logs in accordance with the **ADS 502, The USAID Records Management Program.** At a minimum audit trail records must be maintained online for at least ninety (90) days and preserved for seven (7) years to allow for analysis with reason.

(7) SOs must evaluate the system risks associated with extracts of PII from databases. A sufficiently high risk requires a procedure for logging computer-readable data extracts. The system SSP must document if extract logging is not possible and identify compensating controls.

(8) The CISO must implement both general and threat-specific logging guidance.

545.3.5.4 System and Communications Protection

Effective Date: 11/09/2012

a. Remote Access and Dial-In

System and Communications Protections ensure effective physical and logical network security perimeters and protection of information as it moves within the security perimeter as well as to and from networks outside the security perimeter. Controls for remote access and dial-in include AC, AU, and SC.

The following policy statements apply to remote access and dial-in:

(1) The CISO must develop, disseminate and review/update annually system and communications policy.

(2) SOs must document, implement and enforce procedures to comply with system and communications protection policy and associated system and communications protection controls.

(3) Remote access technology allows trusted employees network entry via dial-in modem or Internet. This enables mobile employees to work away from their central work sites but exposes them to significant security risks. Procedures must mitigate these risks.

(4) Modem connections must be limited because they can circumvent security controls intended to protect USAID networks. Modem connections require CISO authorization. Approved remote access to USAID networks must only be accomplished through equipment specifically approved for that purpose.

(5) Tethering, the connection of two devices via cable or wireless technology for the purpose of accessing the internet through wireless MCDs, requires AO and CISO approval.

(6) The CIO must centrally manage all remote access and dial-in connections to the network and must ensure that remote access and approved dial-in capabilities provide strong authentication, two-factor authentication, audit capabilities, and protection for sensitive information throughout transmission.

(7) Remote access requires two-factor authentication. One factor must be a device separate from the computer gaining access.

(8) Any two-factor authentication requires Agency-controlled certificates or hardware/software tokens issued directly to each authorized user. Remote access solutions must comply with the encryption requirements of **FIPS 14-2, Security Requirements for Cryptographic Modules**. For additional information, please see **Section 545.3.3.11**, **Privacy and Data Security**, for additional requirements involving remote access of PII.

(9) Remote access of PII must comply with all USAID requirements for sensitive systems. This includes including strong authentication, which requires a virtual private network (VPN) or equivalent encryption and two-factor authentication. The Risk Assessment and SSP must document any remote access of PII, approved by the CISO prior to implementation.

(10) Remote access of PII must not permit the download and remote storage of information without addressing requirements for removable media that contains sensitive information. All downloads must follow the concept of least privilege, documented by the SSP.

Please refer to **Guidelines for Remote Access Soft Tokens for Personal Devices**, for information regarding soft token use on personally owned mobile smart devices.

b. Network Security Monitoring

Security Monitoring, Detection and Analysis are key functions and are critical to maintaining the security of USAID information systems. Monitoring and analysis is limited to observing network activity for anomalies, malicious activities and threat profiles. Content analysis is not within the scope of network monitoring. Applicable control includes SI.

The following policy statements apply to network security monitoring:

(1) SOs must provide continuous monitoring of their networks for security events or outsource this requirement to an Agency-approved Security Operations Center (SOC). Monitoring includes interception and disclosure

as required to render service or to protect the Agency's rights or property. Service-observing or random monitoring must not be used except for mechanical or service quality control checks, per the **Electronic Communications Privacy Act**. In this instance, "rights" refers to ownership, entitlements, property, or information as in intellectual property.

(2) The CISO must administer and monitor USAID IDS sensors and security devices.

c. Network Connectivity

System interconnection is the direct connection of two or more information systems to share data and other information resources. This applies to systems which pass data between each other via a direct system-to-system interface without human intervention. It also applies to any physical connection that allows other systems to share data, even if the connected systems do not share data between them. It does not include instances of a user logging on to add or retrieve data, nor users accessing web-enabled applications through a browser. Applicable controls include AC, AU, IA, SC, CM, and CA.

The following policy statements apply to network connectivity:

(1) SOs must ensure appropriate identification and authentication controls, audit logging, and access controls on every network element.

(2) Interconnections between USAID and non-USAID systems must be set through controlled interfaces and via approved service providers. These interfaces must be accredited at the highest security level of information on the network. Interagency Agreements (IAs), Memoranda of Understanding (MOUs), Service Level Agreements (SLAs), or Interconnection Security Agreements (ISAs) must document connections with other Federal agencies. For additional information on MOUs, SLAs, ISAs, or Memoranda of Agreement (MOAs), see **NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems**, or contact the CISO at **isso@usaid.gov**.

(3) SOs must document interconnections between their own and external (Non-USAID) networks with an ISA for each connection.

(4) ISAs require reissue every three (3) years or upon significant changes to interconnected systems.

(5) ISAs require review and update as needed as a part of the annual FISMA self-assessment.

(6) Interconnections between USAID systems require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems. Applicable AO must sign the revised ISA.

(7) The CIO must approve all interconnections between USAID enterprise-level information systems and non-USAID information systems. The CIO must ensure the documentation of connections with other Federal Government Agencies. One ISA may document multiple connections as long as the security categorization and accreditation is the same for all connections covered by that ISA.

(8) The Agency must implement Trust Zones through Policy Enforcement Points (PEPs) as defined by the CISO and CIO.

(9) The CIO must provide secure Name/Address resolution service for all systems connected to the Agency's enterprise network(s).

(10) The appropriate OCIO CCB must update documentation associated with an approved change to an information system to reflect the appropriate baseline.

(11) Interconnections between two accredited USAID systems do not require an ISA if an SSP, SLA, or contract accounts for interface characteristics, security requirements, nature of information communicated, and monitoring procedures for verifying enforcement of security requirements and if AOs accept assessed risks.

(12) Granting the ability to log into one USAID system through another does not require an ISA, provided requirements cited elsewhere in this chapter are met.

d. Internet Protocol Version 6 (IPV6)

Internet Protocol Version 6 provides improved address space, quality of service, and data security over the current IPv4.

The following policies state USAID's position on the transition, implementation and use of IPv6:

(1) The CIO must designate an IPv6 Transition Manager.

(2) The IPv6 Transition Manager leads Agency's IPv6 transition activities and also liaisons with the wider Federal IPv6 effort as necessary.

(3) The CIO must ensure that agency procurements of networked IT satisfy FAR requirements using the USG v6 Profile and Test Program to provide complete and high-quality IPv6 capabilities.

(4) The CIO must upgrade public/external facing servers and services (e.g. Web, e-mail, Domain Name Server (DNS), Internet Service Provider (ISP) services, etc.) to use native IPv6.

(5) The CIO must upgrade internal client applications which communicate with public Internet servers and support enterprise networks to use native IPv6.

e. Firewalls and Policy Enforcement Points

PEPs separate Trust Zones as defined by the CISO and CIO. Firewalls at the TICs and other approved direct-system inter-connections implement boundary protection between USAID and external networks. Applicable controls include AC, SC, MA and IR.

The following policy statements apply to firewalls and policy enforcement points:

(1) SOs must restrict physical access to firewalls and PEP to authorized staff.

(2) SOs must implement identification and strong authentication for administration of firewalls and PEPs.

(3) SOs must encrypt remote maintenance paths to the firewalls and PEPs.

(4) SOs must conduct quarterly firewall and PEP testing to implement the most recent policy changes and to verify that applied policies and controls work.

(5) SOs must ensure that the CISO receives required reports on information security operations status and incident reporting.

(6) All Agency firewalls and PEPs require administration coordinated with USAID security operation capabilities.

(7) All USAID PEPs must provide protection against DOS attacks.

(8) SOs must determine protocols and services permitted through their PEPs.

(9) SOs may restrict traffic sources and destinations at system-level PEPs.

(10) The CISO must establish policy to block or allow traffic sources and destinations at the TIC PEPs.

(11) The CIO must oversee all enterprise PEP activities.

f. Internet Security

Applicable controls include SC, CM, IA, and AC.

The following policy statements apply to internet security:

(1) Any direct connection of USAID networks or USAID mission systems to the Internet or to extranets must occur through USAID PEPs.

(2) Firewalls and PEPs configuration must prohibit any protocol or service not explicitly permitted.

(3) SOs must ensure the OCIO and Program Manager approve all executable code, including mobile code (e.g., ActiveX, JavaScript), prior to code execution within USAID.

(4) Telnet protocol must not be used to connect to any USAID computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, or key exchange), approved by SOs, must be used instead.

(5) File Transfer Protocol (FTP) must not be used to connect to or from any USAID computer. A connection protocol that employs secure authentication (two factor, encrypted, or key exchange), approved by SOs, must be used instead.

(6) Remote Desktop connections, such as Microsoft's Remote Desktop Protocol (RDP), must not be used to connect to or from any USAID computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, or key exchange).

(7) To ensure USAID information and information systems are secure and available, the CIO or CISO, on advice from US-CERT or other reputable

sources, may block specific Internet Web sites or categories at the USAID perimeter.

g. E-mail Security

E-mail allows communication both among USAID staff and outside parties. Improper use of e-mail can disrupt, lose, diminish, or prevent normal workflow. Management must ensure proper e-mail use. SOs must provide appropriate security for their e-mail systems. Applicable controls include SI.

The following policy statements apply to e-mail security.

(1) Staff must follow the standards and procedures in e-mail documentation.

(2) SOs must correctly secure, install, and configure the underlying email operating system.

(3) SOs must correctly secure, install, and configure mail server software.

(4) SOs must secure and filter e-mail content.

(5) SOs must deploy appropriate network protection mechanisms, such as:

- Firewalls,
- Routers,
- Switches, and
- Intrusion detection systems

(6) SOs must secure mail clients to include protection against malware, spyware, and adware.

(7) SOs must conduct mail server administration in a secure manner. This includes:

- Performing regular backups,
- Performing periodic security testing,
- Updating and patching software, and

- Reviewing audit logs at least weekly

(8) USAID e-mail gateways must monitor e-mails for malware at the gateway.

(9) USAID e-mail gateways must monitor e-mails for spam at the gateway.

(10) Auto-forwarding or redirecting of USAID e-mail to address outside of .gov or .mil domains is prohibited. Users may manually forward messages after determining that the risk or consequences are low.

E-mail acceptable use details appear in **E-mail Acceptable Usage Policy**.

h. Personal E-mail Accounts

Only government email accounts should be used transmit official government correspondence. Government accounts will usually end with .gov or .mil extensions. Personal e-mail (.com, .net, .org, etc.) are not authorized to transmit official government correspondence.

The following policy statements apply to personal e-mail accounts:

(1) Staff must follow the standards and procedures outlined in **E-Mail Acceptable Usage Policy.**

(2) The use of personal e-mail accounts (Gmail, Yahoo, and AOL) must not be used to transmit, process, or store Agency-owned information.

(3) Auto-Forwarding or redirecting e-mail to addresses outside of the .gov or .mil domain is prohibited. Users may forward low-risk messages manually.

(4) When sending e-mail to an address outside of the .gov or .mil domain, users must ensure that any sensitive information, particularly PII data elements, is attached as an encrypted file via OCIO-approved encryption technologies. Such transmissions should only be made in the performance of official duties.

i. Vulnerability Management

Vulnerability management consists of detecting, assessing, and mitigating system weaknesses. Information sources include previous risk assessments, audit reports, vulnerability lists, security advisories, and system security testing such as automated vulnerability scanning or security assessments.

Core elements of vulnerability management include continuous monitoring of and mitigating discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk. Applicable controls include SI and RA.

The following policy statements apply to vulnerability management:

(1) SOs must assess sensitive system vulnerabilities annually or whenever significant system changes occur. Assessment includes scanning for unauthorized wireless devices. SARs and annual security control assessments must document annual assessments.

(2) The CISO must approve and manage vulnerability assessments, including assistance in support of incidents resolution, internal and external assessments, and on-going system lifecycle support.

(3) SOs must report compliance with Information System Voice Mail (ISVM) messages within the specified timeframe. SOs unable to meet the designated compliance timeframe must submit documentation of a waiver request via the CISO waiver/exception request process.

(4) The CISO and SOs must be notified before any ISVM scans are run.

(5) The CISO must run periodic scans of all information systems. SOs and/or ISSOs must be notified of such scans.

j. Peer-to-Peer Technology

Applicable controls include CM and SA.

The following statement applies to peer-to-peer technology:

- USAID information systems must not use peer to-peer software unless specifically authorized by the OCIO CCB and the CISO.

545.3.5.5 Cryptography

Effective Date: 11/09/2012

Cryptography converts ordinary text (plaintext) into coded form (ciphertext) by encryption and ciphertext into plaintext by decryption. Cryptography helps add confidentiality, authenticity, and integrity to information.

a. Encryption

Encryption changes plain text into ciphertext for the purpose of security or privacy. Applicable controls include IA and SC.

The following policy statements apply to encryption:

(1) Systems requiring encryption must comply with the following methods: Products using **FIPS 197, Advance Encryption Standard (AES)** algorithms with at least 256-bit encryption validated under **FIPS 140-2**, National Security Agency (NSA) Type 2, or Type 1 encryption.

Note: The use of triple Data Encryption Standard [3DES] and FIPS 140-1 is no longer permitted.

(2) SOs must develop and maintain encryption plans for sensitive information systems requiring encryption.

(3) SOs must use only cryptographic modules that are **FIPS 197** (AES- 256) - compliant and have received **FIPS 140-2**, validation at the level appropriate to their use.

b. Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is an architected set of systems and services to enable the use of public key cryptography. PKI is a requirement for strong security services and for use of digital signatures.

The principal components of a public key infrastructure are the public key certificates, registration authorities (RAs), certification authorities (CAs), directory, certificate revocation lists (CRLs), and a governing certificate policy. Applicable control includes SC.

The following policy statements apply to PKI infrastructure:

(1) The CISO must be the USAID PKI Policy Authority (PKI PA) to provide PKI policy oversight.

(2) The USAID PKI PA must appoint a PKI Management Authority (PKI MA) to provide management and operational oversight of the USAID PKI.

Additional guidance on PKI will appear in a forthcoming Chapter Mandatory Reference. For additional information, direct inquiries to the USAID CISO at **isso@usaid.gov.**

c. Public Key/Private Key

A public key certificate is used to obtain subscribers' public keys in a trusted manner. Once obtained, the public key is then used for the following:

- To encrypt data for that subscriber so that only that subscriber can decrypt it; and
- To verify that the subscriber signed the digitally signed data. This authenticates the identity of the signing subscriber and the integrity of the signed data.

Applicable control includes SC.

The following policy statements apply to public key/private key:

(1) Separate public/private key pairs are a requirement for encryption and digital signature by human subscribers, organization subscribers, application subscribers, and code-signing subscribers.

(2) Separate public/private key pairs are a requirement for encryption and digital signature by device subscribers whenever supported by the protocols native to the type of device.

(3) A human sponsor must represent each application, role, code-signing, and device subscriber during the application process for one or more certificates from a USAID CA.

(4) An authorized USAID employee must sponsor USAID contractors and other affiliates when they apply for one or more certificates from a USAID CA.

(5) Human subscribers must not share private keys and must be responsible for their security and use. If a human subscriber discloses or shares his or her private key, the subscriber must be accountable for all transactions signed with the subscriber's private key.

(6) Sponsors for non-human subscribers (role, application, code-signing, or device) must be responsible for the security of and use of the subscriber's private keys.

(7) CISO must establish a sponsor agreement, and every sponsor must read, understand, and sign the agreement.

(8) Subscriber private keys must not be used by more than one entity unless specifically authorized by the CISO.

545.3.5.6 System and Information Integrity

Effective Date: 11/09/2012

System and Information Integrity is the assurance that the data being accessed or read has neither been tampered with, nor altered, nor damaged. Applicable controls include SI and AC.

The following policy statements apply to system and information integrity:

(1) The CISO must develop, disseminate, and review/update annually a system and information integrity policy.

(2) SOs must document, implement, and enforce procedures to comply with system and integrity policy and associated controls.

(3) SOs must Identify, report, and correct information system flaws; test software updates related to flaw remediation for effectiveness and potential side effects on agency information systems before installation; and incorporate flaw remediation into the configuration management process.

(4) SOs must employ malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or inserted through the exploitation of information system vulnerabilities.

(5) SOs must update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; Configure malicious code protection mechanisms to: Perform periodic scans of the information system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and block malicious code; quarantine malicious code; send alert to system administrator in response to malicious code detection; and address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

(6) SOs must monitor events on the information system in accordance with monitoring objectives and detects information system attacks; Identify unauthorized use of the information system.

(7) SOs must deploy monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.

(8) SOs must heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, or other organizations, based on law enforcement information, intelligence information, or other credible sources of information; and obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

(9) SOs must receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.

(10) SOs must generate internal security alerts, advisories, and directives as deemed necessary; disseminate security alerts, advisories, and directives; and implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

(11) SOs must ensure that the information system detects unauthorized changes to software and information.

(12) SOs must employ spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and update spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

(13) SOs must restrict the capability to input information to the information system to authorized staff.

(14) SOs must ensure that the information system checks the validity of information inputs.

(15) SOs must ensure that the information system identify potentially security-relevant error conditions; generate error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries; and reveal error messages only to authorized staff.

(16) SOs must handle and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

545.3.5.7 Product Assurance

Effective Date: 11/09/2012

Information Assurance (IA) must be a requirement for systems used to input, process, store, display, or transmit sensitive or national security information. IA must be achieved through a strong preference for acquiring and implementing evaluated or validated COTS IA and IA-enabled IT products. These products must provide for system availability. The products must ensure information integrity and confidentiality, as well as authentication and non-repudiation of parties in electronic transactions.

Criteria for these products are as follows:

- The NIST FIPS validation program,
- The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program, and
- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement.

The following policy statements apply to product assurance:

(1) Accredited commercial laboratories or NIST must be conduct evaluation and validation of COTS IA and IA-enabled products.

(2) SOs must use only cryptographic modules that meet the requirements in **Section 545.3.5.5.5, Cryptography.**

(3) Transaction-based systems (e.g., database management systems, transaction processing systems) must implement transaction rollback and transaction journaling, or technical equivalents.

545.3.6 USAID-Specific And Other Policies
Effective Date: 11/09/2012

The following subsections consist of USAID-specific policies and Issue-specific policies, defined as follows:

System-Specific Policies

Analysis of USAID-reported major applications and GSSs identifies system-specific policies. A system-specific policy states information security topics which apply to USAID's information systems, and often addressed the specific context for meeting the security objectives for a given system. The CISO must clear system-specific policies.

Issue-Specific Policies

Issue-specific policies state USAID information security topics for specific Agency areas interest, such as e-mail, internet connectivity, and mobile devices. These issue-specific policies span the entire Agency and often contain unique technology position statements.

545.3.6.1 Pilots, Prototypes, Proof of Concepts
Effective Date: 11/09/2012

The following policy statement applies to pilots, prototypes, and proof-of-concepts:

- Information Systems must have a current ATO, Interim Authorizations to Operate (IATO) are not granted by the Agency and are not recognized by OMB, during pilot phases and must comply with guidance established in the OCIO Standards and Guidelines for Implementing Pilots, Prototypes and Proof of Concepts.

Additional guidance on pilots, prototypes and proof-of-concepts will appear in future guidance. For additional information, contact the CISO at **isso@usaid.gov**.

545.3.6.2 Critical Threat Posts
Effective Date: 11/09/2012

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

The following policy statements apply to critical threat posts:

(1) The mission Executive Officer (EXO) must request that the Regional Security Officer (RSO) perform the highest-level background investigation

available within the host country on all Foreign Service Nationals (FSNs) prior to employment.

(2) FSNs may hold administrative positions that require elevated rights and privileges in critical threat environments.

Note: Critical Threat Missions are defined by the Department of State and are available from the USAID Office of Security.

545.3.6.3 Internet and Intranet Usage

Effective Date: 11/09/2012

The Internet connects computers from around the world, and it 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 in accordance with the Agency's Acceptable Use Policy.

The following policies state USAID's position on the Internet and intranet usage:

(1) The Agency must establish an acceptable use policy for the Internet.

(2) The Agency must establish an acceptable use policy for the intranet.

(3) Specifically prohibited activities, unless approved by OCIO, include but are not limited to, streaming of audio or video; peer-to-peer, software or music sharing/piracy, online gaming visiting, gambling sites, hacking, and the viewing of pornography or other offensive content.

(4) Staff must follow the guidelines outlined in the acceptable use policy for the Internet and intranet: **ROB for Users.**

Additional Internet information is contained in Sections 545.3.4.1 Personnel and 545.3.4.9 Personal Use of Government Office Equipment and USAID Systems/Computers among others and in **Internet Acceptable Usage Policy** and **ADS 541, Information Management**.

545.3.6.4 Internet Radio

Effective Date: 11/09/2012

The following policy statements apply to Internet radio:

(1) Staff must not install or use Internet radio software unless approved by the OCIO CCB and the CISO.

(2) Staff must not use software or web browsers to listen to Internet radio broadcasts unless approved by the OCIO CCB and the CISO.

545.3.6.5 Instant Messaging
Effective Date: 11/09/2012

IM service 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.

The following policy statement applies to instant messaging:

- Staff must not install or use IM software unless approved by the OCIO CCB and the CISO.

545.3.6.6 Mobile Computing Devices
Effective Date: 11/09/2012

Mobile Computing Devices (MCDs) are transportable information processing devices such as laptop computers, PDAs, tablets, smart phones, cell phones, USB drives, and other similar devices. These devices are particularly at risk due to their portability, capacity to store large amounts of data, and monetary value.

MCD users must take extra precautions to compensate for the lack of physical security controls when MCDs lose an information system or transfer data, when access to MCDs originates outside Agency boundaries, or when there is a need to protect MCDs against potential security incidents. Policies are applicable domestically and internationally.

The following policy statements apply to MCDs:

(1) Staff must immediately report the loss or theft of MCDs to the Help Desk.

(2) SOs must encrypt all information stored on government-furnished mobile devices, which must be encrypted in accordance with USAID standards for encryption.

(3) SOs must allow remote access only with two-factor authentication.

(4) SOs must use a “time-out” function for remote access and MCDs requiring user re-authentication after fifteen (15) minutes of inactivity.

(5) All MCDs must employ CISO-approved access control technologies (passwords, PINs, PIV, etc.).

(6) Users must not store database extracts containing SBU to include PII on mobile computing devices.

(7) Staff must follow the respective system and general ROB well as standards and procedures for MCDs.

(8) Staff must not physically connect non-USAID-issued MCDs to the USAID network or information systems.

(9) Staff should backup information often and must only use OCIO-approved backup methods.

(10) Data transfers/transmissions outside of USAID network boundaries must be encrypted if the information contains SBU information and/or PII.

(11) MCDs must not be checked with luggage during travel.

(12) Staff must take all reasonable precautions to protect Agency equipment and information and should ensure that unauthorized persons cannot see information projected on screens.

(13) Staff must not connect USAID-issued MCDs to non-USAID networks or 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.

(14) SAs must securely configure USAID-issued MCDs before connection to the USAID network by means of automated processes such as Network Access Control (NAC). However, when not feasible, the SOs must develop processes and procedures or employ other tools to ensure devices are secure before connection.

Additional guidance on mobile computing is available in **Mobile Computing Standards and Guidelines**.

545.3.6.7 Information Sharing

Effective Date: 11/09/2012

Management must take steps to provide protection for USAID-owned information. These policies cover how to release, if necessary, internal information to internal users

and external parties. Agency staff members are custodians of Privacy and SBU Information.

Information requiring protection includes:

- Information created by, intended solely for, or of sole possession of a single user or group of specified users,
- PII (See **ADS 508**),
- Any information protected under the Privacy Act of 1974,
- Information related to employee health,
- Information protected by Non-disclosure Agreement,
- Agency proprietary information (trade secrets, etc.),
- Executive travel information,
- Procurement-sensitive information,
- Law Enforcement Sensitive
- Information designated as SBU,
- Information designated as For Official Use Only (FOUO), and
- Other information as identified by the information owner, Agency policy or programs.

The following policy statements apply to information sharing:

(1) Staff must process inbound Privacy and FOIA requests through the FOIA Appeals Officer, who uses established rules and procedures to process and provide the requested information;

(2) Staff must coordinate sharing of Privacy information through the Privacy Office;

(3) Staff must protect SBU information leaving Agency boundaries from unauthorized access. These protections should be documented in a memorandum of understanding or agreement;

(4) Staff must protect applicable information in an area guarded by password or other authentication;

(5) Staff must not release their password or other methods of authentication (i.e., keys, access cards, etc.) to unauthorized users; and

(6) Staff must protect sharable information in an area only authorized users can access. Only the SA or network administrator may, upon request, create this storage area using a standard request procedure and upon request delete the area.

Staff must be aware that different types of information require different types of protection and if in doubt contact the CISO for SBU information and the Privacy Office for Privacy information.

The following documents provide related information:

- **ADS 507, Freedom of Information Act**,
- **ADS 508, USAID Privacy Policy**,
- **ADS 509, Creating Altering, or Terminating a System of Records (Records Pertaining to Individuals)**,
- **ADS 557, Public Information**,
- **ADS 559, Inquiries from the News Media**, and
- **ADS 560, News Releases and Services**.

545.3.6.8 Intellectual Property Management

Effective Date: 11/09/2012

Intellectual property is intangible property, such as patents, trademarks, and copyrighted materials which are the result of intellectual effort and is under legal protection. Management must ensure the proper handling of such information.

The following policy statements apply to intellectual property management:

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

(2) Staff using a USAID information system to work with USAID-specific intellectual property must sign a Non-disclosure Agreement (NDA).

(3) Staff using a USAID information system to process or store third-party intellectual property must sign an NDA with the third party when requested.

(4) Staff using, storing, or distributing copyrighted materials on a USAID information system must cite them. Where possible, staff must obtain the permission of the author/owner to use the material.

(5) The CISO, in conjunction with the OCIO, must establish and maintain internal standards for configuration management and procedures for server configuration.

545.3.6.9 Third-Party Web Sites

Effective Date: 11/09/2012

Third-party Web sites are sites funded by the Agency and hosted on environments external to USAID boundaries and not directly controlled by USAID policies and staff, except through the terms and conditions of contracts, grants or cooperative agreements.

The following policy statements apply to the use of third-party Web sites:

(1) **Third-Party Privacy Policies**. Before using any third-party Web site or application to engage with the public, the third party's privacy policy must be examined to evaluate the risks and determine whether the Web site or application is appropriate for the Agency's use. In addition, changes to the third-party's privacy policy must be monitored and risks periodically reassessed.

(2) **External Links**. Posting a link to a third-party Web site or any location not an official Government domain requires an alert to the visitor, such as a statement adjacent to the link or a "pop-up." The alert must explain that the link directs visitors to a non-government Web site where the privacy policies might be different.

(3) **Embedded Applications**. Incorporating or embedding a third-party application on a USAID Web site or in any other Government domain

requires disclosing the third party's involvement and describing the Agency's Privacy Policy.

(4) **Agency Branding**. All websites funded by the Agency must comply with USAID's Agency Branding Standards. (See **Agency Branding Guidelines** and **ADS 320, Branding and Marking**.)

(5) **Information Collection**. When using third-party Web site(s) or application(s), the contractor must collect the least amount of information necessary to complete a function, needed in practice, and called for by statute, regulation, or Executive Order.

545.3.6.10 Cloud Computing

Effective Date: 11/09/2012

Cloud computing, according to NIST, is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. These include networks, servers, storage, applications, and services rapidly provisioned and released with minimal management effort or cloud-provider interaction.

Note: CCB includes CISO approval.

The following policy statements apply to the use of cloud computing:

(1) Cloud computing services must not process production data without written approval from the OCIO and CISO. Required approval may be a security authorization or Authority to Operate, risk decision memorandum based on a risk assessment, and/or OCIO CCB approval.

(2) The Privacy Office must conduct a PIA on information collected.

(3) The CISO must conduct a security categorization of the information types.

(4) The CISO must conduct a risk-based assessment to determine if Agency risk is acceptable for a specific cloud service and if limits are needed.

(5) The CISO must verify that the Agency has approved a Cloud service provider (TOS) agreement before granting cloud service approval.

(6) The CISO must maintain an inventory of approved Cloud services.

(7) The SO must obtain approval from the Office of General Council for a cloud service provider TOS agreement.

(8) The SO, once the CISO approves a cloud service, must create an SLA. There are two types of SLAs for cloud services: predefined non-negotiable service agreement and negotiated service agreement.

(9) Systems containing PII or SBU information must have a negotiated service agreement.

(10) Systems containing non-SBU information may have a predefined non-negotiable service agreement. A predefined non-negotiable service agreement is not suitable for mission critical applications/networks or data.

(11) The COR must ensure that contracts and/or the SLA include the terms and conditions and the responsibilities of the parties for the following issues:

- Regulatory Compliance (NIST/Privacy Act - Security Authorizations),
- Personnel Requirements,
- Data ownership and portability,
- Location of the Agency's data,
- Data Segregation,
- Audit Logs,
- Retention time,
- Records management and electronic discovery,
- Forensics, as well as incident response and reporting,
- System backups,
- Contingency Planning and Disaster Recovery,
- Configuration and Patch Management,
- Security and vulnerability scanning, and

- Agreement termination and data retrieval.

(12) Users must be aware of content, ensure PII and other sensitive information is secure, and safeguard all content from unauthorized disclosure or destruction.

(13) The improper release of PII or other sensitive information may result in civil or criminal penalties, in accordance with the Privacy Act.

(14) Cloud-based computing solutions must comply with guidance supplied by the Federal Risk and Authorization Management Program (FedRAMP) where applicable.

(15) Cloud-based computing solutions must comply with **NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing**.

Refer to the **Contract Clause Guide for Unclassified Information System Security Systems and Services** for additional information.

545.3.6.11 Open Source

Effective Date: 11/09/2012

Source code for open-source software is available for viewing, extension, modification, and perhaps free redistribution. Open-source software is, like freeware, often no cost, but unlike freeware, non-proprietary; i.e., peers can review it.

The following policy statements apply to open source:

(1) Staff must not install open-source software unless approved by the OCIO CCB and the CISO.

(2) If the OCIO or CISO has approved the open-source software but limited or restricted its use, only authorized staff may use it as long as they follow use restrictions and guidelines.

545.3.6.12 Shareware

Effective Date: 11/09/2012

Shareware is software that requires a registration fee. Shareware, like freeware, retains its USAID proprietary character (the fee for use) and like open-source software may include source code distribution. Shareware might contain malicious code.

The following policy statement applies to shareware:

- Staff must not install or use shareware unless approved by the OCIO CCB and the CISO.

545.3.6.13 Freeware
Effective Date: 11/09/2012

Freeware is free software. Freeware, unlike shareware, is largely uncontrolled and proprietary (not subject to source review), and as a result might contain malicious code.

The following policy statement applies to Freeware:

- Staff must not install or use freeware unless approved by the OCIO CCB and the CISO.

545.3.6.14 Remote Control Software
Effective Date: 11/09/2012

Remote control software enables a user to control another user's computer across a network. Remote control software may be bundled with other software, such as collaboration software, file-sharing software, or P2P software.

The following policy statement applies to remote control software:

- Staff must not install or use remote control software unless approved by the OCIO CCB and the CISO.

545.3.6.15 Collaboration Software
Effective Date: 11/09/2012

Collaboration software usually includes file sharing, white-boarding, video- or audio-communication, version control, and document management. It often enables users to connect at two or more devices for concurrent work.

The following policy statements apply to collaboration software:

(1) Staff must not install or use collaboration software unless approved by the OCIO CCB and CISO.

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

545.3.6.16 File-Sharing Software
Effective Date: xx/xx/2012

File-sharing software poses threats to USAID information. They include accidental or deliberate release as well as malicious corruption, alteration, or deletion. File-sharing software may threaten USAID information.

The following policy statement applies to file-sharing software:

- Staff must not install or use file-sharing software unless approved by the OCIO CCB and the CISO.

545.4 MANDATORY REFERENCES

This section contains references, including external and internal mandatory references, which shape the Agency's security stance and policy.

545.4.1 External Mandatory References
Effective Date: 11/09/2012

545.4.1.1 Federal Statutes
Effective Date: 11/09/2012

a. **Federal Acquisition Regulation (FAR)**

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

c. **Public Law 93-579, The Privacy Act of 1974, 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** [To obtain this document, please contact **ads@usaid.gov**]

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)

Effective Date: 11/09/2012

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

545.4.1.3 Memoranda
Effective Date: 11/09/2012

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)
Effective Date: 11/09/2012

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)
Effective Date: 11/09/2012

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

545.4.1.6 National Strategy
Effective Date: 11/09/2012

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

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

545.4.1.7 Homeland Security Presidential Directive (HSPD)
Effective Date: 11/09/2012

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)**

545.4.1.8 NIST Special Publications
Effective Date: 11/09/2012

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, Guidelines 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 (rev. 1), Guide to Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

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, Guidelines 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, Rev. 3, 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**

aaa. **NIST Description, The United States Government Configuration Baseline (USGCB), March 7, 2010**

bbb. **USGCB Highlights CIO Council, US Government Configuration Baseline (USGCB) Highlights, September 15, 2010**

545.4.1.9 NIST Federal Information Processing Standards (FIPS)
Effective Date: 11/09/2012

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

b. **FIPS PUB 140-1, Security Requirements for Cryptographic Modules, January 1994**

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

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

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

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

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

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

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

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

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

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

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

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

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

545.4.1.10 Office of Management and Budget (OMB)
Effective Date: 11/09/2012

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

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

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**

545.4.1.11 Presidential Memoranda

Effective Date: 11/09/2012

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

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

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

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

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

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

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

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

545.4.2 Internal Mandatory References

Effective Date: 11/09/2012

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

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

c. **ADS 508, The USAID Privacy Policy**

d. ADS 541, Information Management

e. ADS 545mai, Business Continuity Planning Procedures and Guidelines

f. ADS 545mak, Data Remanence Procedures

g. ADS 545mal, Disaster Recovery Planning Procedures and Guidelines

h. ADS 545mam, E-Mail Acceptable Usage Policy

i. ADS 545man, Establishing System Security Level Procedures and Guidelines

j. ADS 545map, Incident Identification and Reporting Procedures

k. ADS 545maq, Information Assurance Procedures

l. ADS 545mar, Internet Acceptable Usage Policy

m. ADS 545mas, Media Handling Procedures and Guidelines

n. ADS 545mat, Mobile Computing Standards and Guidelines

o. ADS 545mau, Password Creation Standards and Technical Controls

p. ADS 545max, Restricted Access Procedures and Guidelines

q. ADS 545may, Risk Assessment Guidelines

r. ADS 545maz, ROB for Executive Management

s. ADS 545mba, ROB for Functional Management

t. ADS 545mbb, ROB for ISSOs

u. ADS 545mbc, ROB for System Administrators

v. ADS 545mbd, ROB for Users

w. ADS 545mbf, Virus Detection Guidelines

x. ADS 545mbg, Wireless Access Standards and Guidelines

y. **ADS 545mbm, Guidelines for Remote Access Soft Tokens for Personal Devices**

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

aa. **ADS 557, Public Information**

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

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

dd. **USAID ADS Acquisition and Assistance Series**

ee. **Computer Security User Account Management Procedures** [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.]

ff. **Incidence Response Guidance for Unclassified Information Systems** [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.]

gg. **USAID FISMA Program Guide** [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.]

hh. **USAID Incident Handling Guide** [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.]

ii. **USAID Plan of Action and Milestones (POA&M) Process Guide** [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.]

jj. **USAID Secure Baseline Configuration Guide** [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.]

kk. **USAID Security Authorization Process Guide** [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.]

ll. **USAID Vulnerability Management Guide** [Please contact the Information Assurance Division at **isso@usaid.gov** for a copy of this document.]

545.4.3 Mandatory Forms
Effective Date: 11/09/2012

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)

545.5 ADDITIONAL HELP
Effective Date: 11/09/2012

a. **ADS 545sah, Warning Screen Messages Guidelines**

b. **IDmanagement.gov**

545.6 DEFINITIONS
Effective Date: 11/09/2012

This section defines terms including acronyms used in this document. For additional definitions, please see the **ADS Glossary**.

802.11
The term 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)

Advanced Encryption Standard (AES)
Products using **FIPS 197, Advance Encryption Standard (AES)** algorithms with at least 256-bit encryption validated under **FIPS 140-2**, National Security Agency (NSA) Type 2, or Type 1 encryption.

audit
An independent review and examination of system records and activities. (Chapter 545)

Authority to Operate (ATO)
The formal declaration by the DAA that an Information System is approved to operate using a prescribed set of safeguards.

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

Authorizing Official (AO) (or designated approving/accrediting authority)
A senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. (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**)

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)

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)

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)

Capital Planning and Investment Control (CPIC)
A decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. (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 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 DAA. (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)

Chief Information Security Officer (CISO)
The CISO, 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 Agency information security/assurance matters. (Chapter 545)

Chief Privacy Officer (CPO)
The individual who has overall Agency responsibility for policy development, oversight, and implementation of an agency-wide privacy program. (Chapter 545)

Chief Information Officer (CIO)
The CIO is an organizational official responsible for: (i) designating a senior information security officer; (ii) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements; (iii) overseeing personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained; (iv) assisting senior organizational officials concerning their security responsibilities; and (v) in coordination with other senior officials, reporting

annually to the head of the federal agency on the overall effectiveness of the organization's information security program, including progress of remedial actions. (Chapter 545)

Commercial-off-the-Shelf (COTS)
A FAR term defining a non-developmental item (NDI) of supply that is both commercial and sold in substantial quantities in the commercial marketplace, and that can be procured or utilized under government contract in the same precise form as available to the general public. (Chapter 545)

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 (CM)
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)

Configuration Management Plan (CMP)
A plan that establishes and maintains consistency of a product's performance and functional and physical attributes with its requirements, design, and operational information throughout its life. (Chapter 545)

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

Continuity of Operations Planning (COOP)
A plan to test, implement, and maintain the continuity and recovery of essential USAID functionality. (Chapter 545)

Contractor
This term refers to an U.S Citizens who are employed as Personal Service Contractors (PSC), independent contractor, fellow, institutional contractor, or any other category of individual, not a direct-hire, requiring a security clearance to work on USAID information or material or have unescorted access in USAID space. (Chapters 545, **567**)

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 mission/post
This term refers to those missions/posts that are defined by the Department of State and are available from the USAID Office of Security. These missions/posts are often located in regions where excessive local threats such as social, political and natural disasters are likely to occur. (Chapter 545)

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

Denial-of-Service (DOS)
A DOS attack is an attack designed to make a resource unavailable to its intended users. (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 without the possibility of harm to any production system. (Chapter 545)

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)

Domain Name Server (DNS)
A server that hosts a network service for providing responses to queries against a directory service. It maps a human-recognizable identifier to a system-internal, often numeric, identification or addressing component. This service is performed by the server according to a network service protocol. (Chapter 545)

Dynamic Host Configuration Protocol (DHCP)
A protocol that allows client devices to request IP addresses from a DHCP server as needed (Chapter 545)

employee
The term “employee” Includes all USAID U.S. citizen direct-hire personnel, Personal Service Contractors (PSC) and Participating Agency Staff (PASA). (Chapter 545)

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

exception
An exception is an authorization to proceed outside of policy when certain conditions apply. (Chapter 545)

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

Executive Officer (EXO)
Unit Security Officer, responsible to both SEC and the post RSO, ensuring USAID compliance with USAID and Post security directives (Chapters 545, **527**, **535**)

Executive Order (EO)
A rule or order having the force of law, issued by the President of the United States. (Chapter 545)

External Services
These include services that are provided to the Agency and are under contract and funded by the Agency. (Chapter 545)

External System
These include systems that are **not** part of, connected to, operated or owned by the Agency. These are systems that are under contract to, funded by and operated on behalf of the Agency. (Chapter 545)

Federal Acquisition Regulation (FAR)
The principal set of rules in the Federal Acquisition Regulation System. This system consists of sets of regulations issued by agencies of the federal government of the United States to govern the acquisition process. This is the process through which the government purchases (acquires) goods and services. (Chapters 545, **302**, **330**)

Federal Desktop Core Configuration (FDCC)A list of security settings recommended by the National Institute of Standards and Technology for general-purpose microcomputers connected directly to the network of a United States government agency. (Chapter 545)

Federal Information Processing Standards (FIPS)
A publicly announced standardization developed by the United States federal government for use in computer systems by all non-military government agencies and by government contractors, when properly invoked and tailored on a contract. (Chapter 545)

Federal Information Security Management Act of 2002 (FISMA)
(44 U.S.C. § 3541, et seq.), a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899). The act recognizes the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. (Chapter 545)

Federal Risk and Authorization Management Program (FedRAMP)
A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. (Chapter 545)

File Transfer Protocol (FTP)
File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet. (Chapter 545)

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

Freedom of Information Act (FOIA)
A federal freedom of information law that allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States government. The Act defines agency records subject to disclosure, outlines mandatory disclosure procedures, and grants nine exemptions to the statute. (Chapters 545, **557**)

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 Services Administration (GSA)
An independent agency of the United States government, established in 1949 to help manage and support the basic functioning of federal agencies - The GSA supplies products and communications for U.S. government offices, provides transportation and office space to federal employees, and develops government-wide cost-minimizing policies, and other management tasks. (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 shared information processing service organization. (Source: **NSTISSI 1000** and **OMB Circular A-130**) (Chapter 545)

Government Information Security Reform Act (GISRA)
A federal law that requires U.S. government agencies to implement an information security program that includes planning, assessment, and protection. It was enacted in 2000 and replaced by FISMA in 2002. (Chapter 545)

Heating, Ventilation, and Air Conditioning (HVAC)
This combines three functions into one system. Warmed or cooled or dehumidified air flows through a series of tubes - called ducts – for distribution through a building. (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)

Identity, Credentialing, and Access Management (ICAM)
ICAM represents the intersection of digital identities (and associated attributes), credentials, and access control into one comprehensive approach. (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)

independent assessor
This refers to individuals(s) who have no vested interested in a system or process and who are not in the same chain of authority as the system they are assessing. (Chapter 545)

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

Information Assurance (IA)
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 Security Vulnerability Management (ISVM)
The cyclical practice of identifying, classifying, remediating, and mitigating information security vulnerabilities. (Chapter 545)

Information System (IS)
A discrete set of information resources organized to collect, process, maintain, use, share, disseminate, or dispose of information. (Source: **NIST SP 800-18**) (Chapter 545)

Information Systems Security Officer (ISSO)
Individual responsible to the senior agency information security officer, AO, or information SO 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)

Instant Messaging (IM)
A form of communication over the Internet that offers instantaneous transmission of text-based messages from sender to receiver. (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, and copyrights. (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 1000**) (Chapter 545**)**

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

Internet Protocol Version 6 (IPV6)
IPv6 (Internet Protocol version 6) is a set of specifications from the Internet Engineering Task Force (IETF) that is not only an upgrade but a replacement for IP version 4 (IPv4). Both refer to the standard used in addressing information systems, computers and other similar devices to facilitate the transmission and reception of information. (Chapter 545)

Internet Service Provider (ISP)
Commonly called ISP, this term refers to any, organization, company or source for the provision of a connection to the internet to anyone, any organization or company. (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
These 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)

Joint Worldwide Intelligence Communications System (JWICS)
A system of interconnected computer networks primarily used by the United States Department of Defense, United States Department of State, United States Department of Homeland Security, and the United States Department of Justice to transmit classified information by packet switching over TCP/IP in a secure environment. (Chapter 545)

Land Mobile Radio (LMR)
A wireless communications system intended for use by terrestrial users in vehicles (mobiles) or on foot (portables). Such systems are used by emergency first responder organizations, public works organizations, or companies with large vehicle fleets or numerous field staff. Such a system can be independent, but often can be connected to other fixed systems such as the public switched telephone network (PSTN) or cellular networks. (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 IS. (Chapter 545)

least required functionality
This refers to activating or making only those functions available necessary to achieve or support a business need. (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 Circular A-130**) (Chapter 545)

managerial controls
Security methods that focus on mechanisms that are primarily implemented by management staff. (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: CD-ROMs, tapes, diskettes, disk drives, memory sticks, and others. (Chapter 545)

Memorandum of Agreement (MOA)
Documents outlining the cooperative terms, responsibilities, and often funding of two entities to work in partnership on certain listed projects. The agreed responsibilities of the partners will be listed and the benefits of each party will be listed. (Chapter 545)

Mobile Computing Device (MCD)
A small, hand-held computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds (0.91 kg). (Chapter 545)

Multimedia Messaging Service (MMS)
A standard way to send messages that include multimedia content to and from mobile phones. It extends the core SMS capability that allows exchange of text messages only up to 160 characters in length. (Chapter 545)

National Archives and Records Administration (NARA)
An independent agency of the United States government charged with preserving and documenting government and historical records and with increasing public access to those documents, which comprise the National Archives. NARA maintains and publishes the legally authentic and authoritative copies of acts of Congress, presidential proclamations and executive orders, and federal regulations. (Chapters 545, **502**)

National Institute of Standards and Technology (NIST)
A non-regulatory federal agency within the U.S. Department of Commerce. The NIST mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. (Chapter 545)

National Security Agency (NSA)
A cryptologic intelligence agency of the United States Department of Defense responsible for the collection and analysis of foreign communications and foreign signals intelligence, as well as protecting U.S. government communications and information systems. This involves information security and cryptanalysis/cryptography. (Chapter 545)

need to know
The need for specific information not normally available without 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)

Network Access Control (NAC)
An approach to computer network security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication, and network security enforcement. (Chapter 545)

Non-Disclosure Agreement (NDA)
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. (Chapter 545)

Office of Foreign Disaster Assistance (OFDA)
An organizational unit within USAID that directs and coordinates international United States government disaster assistance. (Chapter 545)

Office of Personnel Management (OPM)
A U.S. government agency that recruits, retains, and honors a workforce to serve the American people. (Chapter 545)

Office of Security (SEC)

A USAID business unit that provides physical security services to protect USAID personnel and facilities, safeguard national security information. (Chapter 545)

Office of the Chief Information Officer (OCIO)
The USAID business unit that supports the CIO and that comprises the CIO staff. (Chapter 545)

Office of the Inspector General (OIG)
This office oversees USAID's statutory responsibilities regarding FISMA and other statutory and regulatory guidance for information security. (Chapter 545)

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

Participating Agency Service Agreements (PASA)
PASAs are agreements between US government agencies in which staff are basically seconded or assigned from their agency to work on project-specific tasks. Sometimes contractors under these agreements may be referred to as PASAs. (Chapter 545)

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

Personal Digital Assistants (PDAs)
This is a term for any small mobile hand-held device that provides computing and information storage and retrieval capabilities. A PDA is a Mobile Computing Device (MCD). (Chapter 545)

Personal Service Contractor (PSC)
This term refers to a type of contractor who provides specialized technical assistance in designing and managing programs, primarily in the field. They can be locally recruited or internationally recruited. (Chapter 545)

Personally Identifiable Information (PII)
This refers to information that directly identifies an individual. PII examples include name, address, social security number, or other identifying number or code, telephone number, and e-mail address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. Same as "information in an identifiable form". (Chapters 545, **508**)

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)

Personal Identity Verification (PIV)
The identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201 specifies PIV requirements for Federal employees and contractors. (Chapter 545)

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

Plan of Action and Milestones (POA&M)
According to OMB M-02-01, a POA&M identifies tasks to do. It details resources to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. A POA&M assists agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. (Chapter 545)

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

Policy Enforcement Point (PEP)
A firewall or similar device that can be used to restrict information flow. (Chapter 545)

port
Used in this document to denote a place where one might connect a computer to a network. (Chapter 545)

Privacy Impact Assessment (PIA)
Analysis of how information is handled:1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in electronic information systems, and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. (Chapters 545, **508**)

Privacy Threshold Assessment (PTA)
A Privacy Threshold Assessment or Analysis (PTA) provides a high-level description of an information system including the information it contains and how it is used. The PTA determines and documents whether or not a PIA and/or SORN is required. (Chapters 545, **508**)

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, 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 (PM)
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
These 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)

Public Key Infrastructure (PKI)
A set of hardware, software, people, policies, and procedures which create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). (Chapter 545)

Radio Frequency Identification (RFID)
The use of a wireless non-contact system employing radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking. (Chapter 545)

RATO
A legally binding written permission to conduct activities but under certain restrictions (Chapter 545)

Record Retention Standard (RRS)
An aspect of records management that specifies the policy controlling how long a record must be kept. (Chapter 545)

Regional Security Officer (RSO)
Are Department of State, Bureau of Diplomatic Security Special Agents. They are responsible to the Chief of Mission at US posts abroad. The RSO also receives management direction from Diplomatic Security through the Assistant Director for International Programs (DS/DSS/IP). (Chapter 545)

Registration Authorities (RAs)
Register and administer identifiers used in information technology. (Chapter 545)

Remote Desktop Protocol (RDP)
This provides a user with a graphical interface to another computer. (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 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 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 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 accreditation
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. (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, Vol. I**, **FIPS 199**) (Chapter 545)

Sensitive Compartmentalized Information (SCI)
The term refers to a method of handling certain types of classified information that relate to specific national security topics or programs whose existence is not publicly acknowledged, or the sensitive nature of which requires special handling. (Chapter 545)

Secure Shell (SSH)
A cryptographic network protocol for secure data communication, remote shell services, or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server and a client (running SSH server and SSH client programs, respectively). The protocol specification distinguishes two major versions that are referred to as SSH-1 and SSH-2. (Chapter 545)

Security Operations Center (SOC)
A centralized unit in an organization that deals with security issues, on an organizational and technical level. An SOC within a building or facility is a central location from where staff supervises the site, using data processing technology. Typically, it is equipped for access monitoring, and controlling of lighting, alarms, and vehicle barriers. (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 1000**) (Chapter 545)

Senior Agency Information Security Officer (SAISO)

The Senior Agency Information Security Officer (or senior information security officer) is an organizational official responsible for: (i) carrying out the CIO security responsibilities under FISMA; and (ii) serving as the primary liaison for the CIO to the organization's AOs, information SO, common control providers, and ISSOs. The senior information security officer: (i) possesses professional qualifications, including training and experience, required to administer the information security program functions; (ii) maintains information security duties as a primary responsibility; and (iii) heads an office with the mission and resources to assist the organization in achieving more secure information and information systems in accordance with the requirements in FISMA. The senior information security officer (or supporting staff members) may also serve as AO designated representatives or security control assessors. The role of senior information security officer has inherent U.S. Government authority and is assigned to government personnel only. The SAISO in USAID is the CISO. (Chapter 545)

Sensitive But Unclassified (SBU)
SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: **The Freedom of Information Act**, **The Privacy Act** , **12 FAM 540, Sensitive But Unclassified Information**, (TL;DS-61;10-01-199), and **12 FAM 541 Scope** (TL;DS-46;05-26-1995). (Chapter 545)

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.

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)

Short Message Service (SMS)
A text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. (Chapter 545)

Social Security Number (SSN)
A nine-digit number issued by the Social Security Administration to U.S. citizens, permanent residents, and temporary (working) residents under section 205(c)(2) of the Social Security Act, codified as 42 U.S.C. § 405(c)(2). Its primary purpose is to track individuals for Social Security purposes. (Chapter 545)

Special Publication (SP)
A document, published by NIST, of general interest to the computer security community. (Chapter 545)

staff
The term "staff" refers to any USAID employee, contractor, Foreign Service National (FSN) 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)

Statement of Work (SOW)
A formal document that captures and defines the work activities, deliverables, and timeline a vendor must execute in performance of specified work for a client. The SOW usually includes detailed requirements and pricing, with standard regulatory and governance terms and conditions. (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)
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 (SDLC)
The process of developing information systems through investigation, analysis, design, implementation, and maintenance. (Chapter 545)

System of Records Notices (SORNs)
A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. (Chapter 545)

System Owner (SO)
Individual responsible for daily program and operational management of their specific USAID system. SOs 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 A&A. It is a representation of a system through which the A&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)

Tethering
The connection of two devices via cable or wireless technology for the purpose of accessing the internet through wireless Mobile Computing Devices (MCDs). (Chapter 545)

Telework
This refers to the act of working off-site, generally from home, by accessing Agency systems remotely. (Chapters 545, **405**)

Terms of Service (TOS)
Also known as Terms of Use and Terms & Conditions are rules which one must agree to abide by in order to use a service. Sometimes used as a Disclaimer, especially regarding the use of websites. (Chapter 545)

third-party
The term refers to any non-Agency staff. (Chapter 545)

third-party web sites
Sites hosted on environments external to USAID boundaries and not directly controlled by USAID policies and staff, except through the terms and conditions of contracts, grants or cooperative agreements. (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 DOS. (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)

TOP SECRET (TS)
A security clearance affording access to data that affects national security, counterterrorism/counterintelligence, or other highly sensitive data. (Chapter 545, **552**)

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)

Triple Data Encryption Algorithm (TDEA)
In cryptography the block cipher that applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. (Chapter 545)

Triple Data Encryption Standard (TDES)
The common name for TDEA. (Chapter 545)

Trust Framework Provider Adoption Process (TFPAP)
A process whereby the government can assess the efficacy of the Trust Frameworks so that an Agency online application or service can trust an electronic identity credential provided to it at a known level of assurance comparable to one of the four OMB Levels of Assurance. Trust Frameworks that are comparable to federal standards are adopted through this process, allowing federal relying parties to trust credential services that have been assessed under the framework. (Chapter 545)

unclassified information
Information that has not been determined, per **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. (Source: **ADS 552**) (Chapter 545)

United States Computer Emergency Readiness Team (US-CERT)
Part of the National Cyber Security Division of the United States' Department of Homeland Security**,** US-CERT serves as the focal point for cybersecurity issues in the United States. US-CERT is a partnership between the Department of Homeland Security and the public and private sectors, intended to coordinate the response to security threats from the Internet. As such, it releases information about current security issues, vulnerabilities and exploits via the National Cyber Alert System and works with software vendors to create patches for security vulnerabilities. (Chapter 545)

United States Government Configuration Baseline (USGCB)
An initiative to create security configuration baselines for IT products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate and provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. (Chapter 545)

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 term “user” or “users” refers to any staff member with authorized access to USAID‘s information systems. A user can also be someone who uses information processed by USAID‘s information systems and may have no access to USAID‘s information systems. (Chapter 545)

user classifications
NIST SP 800-16 defines five user classifications: Users, Systems Administrators, ISSOs, 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 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 1000**) (Chapter 545)

Virtual Private Network (VPN)
A technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks otherwise inaccessible. A VPN provides security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network. VPNs can connect individual users to a remote network or connect multiple networks together. (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
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 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 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)

Wireless Local Area Network (WLAN)
A WLAN links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet. (Chapter 545) **Check Glossary

Wireless Personal Area Network (WPAN)
A computer network used for communication among computerized devices carried over wireless network technologies. Can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink). (Chapter 545)

Wireless Wide Area Network (WWAN)
A form of wireless network. The larger size of a wide area network compared to a local area network requires differences in technology. Wireless networks of all sizes deliver data in the form of telephone calls, web pages, and streaming video. A WWAN often differs from wireless local area network (WLAN) by using mobile telecommunication cellular network technologies to transfer data. It can also use Local Multipoint Distribution Service (LMDS) or Wi-Fi to provide Internet access. These technologies are offered regionally, nationwide, or even globally and are provided by a wireless service provider. WWAN connectivity allows a user with a laptop and a WWAN card to surf the web, check email, or connect to a VPN from anywhere within the regional boundaries of cellular service. (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)

Voice over Internet Protocol (VoIP)
Voice over Internet Protocol refers to the communications protocols, technologies, and methodologies used to deliver voice communications over Internet Protocol (IP) networks. (Chapter 545)

545_110912