
# ADS Chapter 545

# Information Systems Security

Full Revision Date: 10/10/2017
Responsible Office: M/CIO/IA
File Name: 545_101017

**Functional Series 500 – Management Services**
**ADS 545 – Information Systems Security**
**POC for ADS 545: Bruce Wierzechowski, (202) 657-1878,**
**bwierzechowski@usaid.gov**

***This chapter has been revised in its entirety.***

## Table of Contents

# ADS 545 – Information Systems Security

## 545.1 OVERVIEW
Effective Date: 10/10/2017

The **Federal Information Security Modernization Act of 2014** (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems (ISs) that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. USAID has developed policies and standards, outlined in this document, to comply with FISMA and to provide secure Information Technology (IT) services to facilitate USAID's mission.

This policy applies to all USAID staff and IT services, ISs, and information owned by or operated on behalf of USAID. It is designed to protect the Agency's IT assets and information from unauthorized access, use, disclosure, disruption, modification, and/or destruction.

Applicability Statement: Throughout this chapter, the term "workforce" refers to individuals working for or on behalf of the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems. This includes Direct-Hire employees, Personal Services Contractors, Fellows, Participating Agency Service Agreement and contractor personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS Chapter 501**. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to HSPD-12 and Information Security requirements.

The standards established in this ADS chapter represent the minimum standards for information systems security for a USAID IS, in accordance with **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4**. However, when an information system is categorized as Low or High for security impact, these standards will be tailored in accordance with minimum security controls as defined by NIST SP 800-53, Revision 4, for the specific security categorization.

Refer to **ADS 552, Classified Information Systems Security** for compliance requirements for classified ISs.

Any specific responsibilities for risk management mentioned in this ADS chapter will be exercised consistent with the Agency Enterprise Risk Management governance structure detailed in **ADS 596mab**.

## 545.2 PRIMARY RESPONSIBILITIES
Effective Date: 10/10/2017

All government offices, United States Direct-Hires (USDH), and other employees bear the primary responsibilities for information systems security. Although contractors, Personal Service 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 otherwise stated, security specific roles must be filled by USDH personnel.

**a.** The **Administrator** is responsible for providing information security protections for the Agency. 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; and

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

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

**c.** The **Chief Information Security Officer (CISO)** is the Agency's senior information security official. The CISO:

**1)** Carries out CIO security responsibilities under FISMA;

**2)** Carries out Risk Executive functions for the Agency;

**3)** Serves as the primary liaison for the CIO to USAID's Authorizing Officials (AOs), Information System Owner (SO), common control providers, and Information System Security Officers (ISSOs). The CISO (or supporting staff members) may also serve as an AO-designated representative or security control assessor; and

**4)** Ensures promulgation and enforcement of the policy in this chapter.

**d.** The **Chief Privacy Officer (CPO)** is responsible for establishing strategic direction and maintaining oversight of the USAID Privacy Program to ensure that it is in compliance with all applicable statutory and regulatory guidance. This includes reviewing privacy compliance documentation (including privacy threshold analyses (PTAs), privacy impact assessments (PIAs), Privacy Act system of record notices (SORNs), and privacy statements for Web sites and forms) must be approved by the CPO and his/her staff prior to a system receiving an authority to operate (ATO). The CPO is responsible for

managing responses to incidents involving Personally Identifiable Information (PII or other sensitive information), and for privacy-related issues and responses to audits and program reviews.

**e.** The **Senior Accountable Official for Risk Management (SAORM)** has Agency-wide responsibility and accountability for implementation of USAID's cybersecurity risk management measures. These responsibilities include ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes in accordance with chapter 35, subchapter II, of title 44, United States Code (USC).

**f.** The **Senior Agency Official for Privacy (SAOP)** has overall responsibility and accountability for working with the CPO to ensure the Agency's implementation of information privacy protections and Agency compliance efforts. These responsibilities include ensuring full Agency compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act. The SAOP is also responsible for evaluating the privacy impact of all new technology and its impact on PII. The SAOP manages the Agency's response to Office of Management and Budget (OMB)/ Department of Homeland Security (DHS) reporting requirements. The SAOP is also responsible for ensuring that all staff receives the appropriate privacy training, both annual and role-based.

**g.** The **Information Owner (IO)** is an Agency official that has been given 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 SO.

**h.** The **Business Owner** has varying responsibilities depending on the Mission or Business or Information Owner. In general, Business Owners are responsible for ensuring the mission of the organization is accomplished. In some cases, Business Owners are responsible for funding and other resources that support their line of business.

**i.** 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, and other organizations. Only the AO may officially accept risks on behalf of the Agency. The AO must be separate from the system owner (SO) and must not hold any other significant security role for a system for which the AO role is also held. 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 CIO, CISO, Common Control Providers, SOs, ISSOs, security control assessors, and other stakeholders during the security authorization process.

**j.** The **Designated Authorizing Official Representative (DAOR)** 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. There are two actions that cannot be

delegated to the DAOR: signatures for system ATO and signatures for formal risk decision memorandums (i.e., the acceptance of risk to Agency operations and assets, individuals, and other organizations).

**k.** 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 the following:

**1)** Documenting the organization-identified common controls in a security plan (or equivalent document prescribed by the organization);

**2)** Ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization;

**3)** Maintaining 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 SOs inheriting those controls after the information is reviewed and approved by the senior official or executive with oversight responsibility for those controls; and

**4)** Remediating weaknesses identified for associated common controls.

**l.** The **System Owner (SO)** is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The SO must maintain a separation of duties from the AO, and must not hold any other significant responsibility for a system for which an AO role is also held.

**m.** 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, i.e., instruction in Rules of Behavior (ROB).

For the Missions, the role of System Owner (SO) is filled by the Mission Information Systems Security Officer (ISSO) (usually a Mission’s Executive Officer (EXO), who must be a member of USDH staff). M/CIO provides onsite training to ISSOs and EXOs filling

that role.

**n.** 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. The ISSO may be a non-USDH staff member, but the ISSO must be a cleared U.S. citizen with a clearance at least equal to the highest security classification of the information being protected.

**o.** 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 (ISs) supporting those missions and business processes.

**p.** 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 (i.e., integrated project team) designing and developing organizational information systems or upgrading legacy systems.

**q.** 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 provide an assessment of the weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. Results of the assessment must be documented in a security assessment report.

## 545.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 10/10/2017

Information security policies delineate the security management structure and foundation to measure progress and compliance. The CISO maintains the policies in this ADS chapter and may alter the policies 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.

At the discretion of the Administrator (A/AID) or designees, certain USAID Security Authorization roles may be delegated (i.e., role representatives) and, if so, must be documented and maintained on file as part of the official record. 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).

Please note: Sections **545.3.1** through **545.3.18** correspond to required security controls, per **NIST 800-53, rev 4**. The abbreviation following each section heading includes the identifier for that control (i.e, PM for Program Management, AC for Access Control, AT, for Awareness and Training, etc).

### 545.3.1 Program Management (PM)

#### 545.3.1.1 Information Security Program Plan (PM-1)

Effective Date: 10/10/2017

The Chief Information Security Officer (CISO) must develop, document, disseminate, protect, review annually, and update as required, 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.** Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

**c.** Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and

**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, and individuals.

#### 545.3.1.2 Senior Information Security Officer (PM-2)

Effective Date: 10/10/2017

The Chief Information Officer (CIO), or designee, must appoint an experienced Senior Information Security Officer or Chief Information Security Officer with the responsibility for the development, management, and implementation of the Information Security Program Plan.

#### 545.3.1.3 Information Security Resources (PM-3)

Effective Date: 10/10/2017

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; employ a business case to record the resources required;

and ensure that information security resources are available for expenditure as planned. System Owners (SOs), Business Owners, or Authorizing Officials (AOs) are responsible for ensuring these requirements are met for all IT assets deployed for Agency operations. For details, see **ADS 542, Planning and Budgeting for Information Technology (IT) Resources**, **ADS 547, Property Management of Information Technology (IT) Resources**, **ADS 562, Physical Security Programs (Overseas)**, **NIST SP 800-65**, and **OMB Exhibit 300**.

#### 545.3.1.4 Plan of Action and Milestones Process (PM-4)

Effective Date: 10/10/2017

The CISO must:

**a.** Implement a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are developed and maintained;

**b.** Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the nation, and report these actions in accordance with OMB FISMA reporting requirements; and

**c.** Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

For more information, please see USAID POA&M Management Guide, USAID FISMA Program Guide and Documenting Security Weaknesses in a POA&M. To obtain copies of these documents, go to **https://pages.usaid.gov/M/CIO/security-assessment-and-authorization-saa** or send an email to **ato@usaid.gov**.

#### 545.3.1.5 Information System Inventory (PM-5)

Effective Date: 10/10/2017

The Bureau for Management, Office of the Chief Information Officer (M/CIO) must develop and maintain an inventory of Agency information systems, including approved social media sites and cloud-based systems/services. The Chief Financial Officer (CFO) must maintain an inventory of all Agency Financial Management Systems. The CISO must maintain an inventory of all FISMA reportable information systems.

#### 545.3.1.6 Information Security Measures of Performance (PM-6)

Effective Date: 10/10/2017

The CISO must develop, monitor, and report the results of information security measures of performance as part of the Agency Information Security Program. Reporting must include outcome-based metrics demonstrating the effectiveness of security controls in use, which includes periodic OMB FISMA data collected from SOs. For more information, see **NIST SP 800-55**.

### 545.3.1.7 Enterprise Architecture (PM-7)
Effective Date: 10/10/2017

M/CIO must develop an enterprise architecture integrated with information security at an organization-wide level. This information security architecture must address risk to Agency individuals, assets, and operations while protecting Agency core missions and business processes and aligning with Federal Enterprise Architecture to protect other organizations and the nation. For details, see **OMB Enterprise Architecture Assessment Framework** and the **M/CIO Strategic Planning and Enterprise Architecture**.

### 545.3.1.8 Critical Infrastructure Plan (PM-8)
Effective Date: 10/10/2017

If the USAID Administrator officially declares that the Agency mission includes Critical Infrastructure, M/CIO (or other designees) has specific responsibilities. In coordination with the CISO and based on priority strategy, guidance, and the Risk Management Framework, M/CIO must address information security issues when developing, documenting, and updating the critical infrastructure. This includes creation of a key resources protection plan. For more information, contact **ato@usaid.gov**.

### 545.3.1.9 Risk Management Strategy (PM-9)
Effective Date: 10/10/2017

M/CIO must develop, implement, review annually and update as required an Agency-wide risk management strategy to protect information assets. M/CIO must provide sufficient resources to implement the risk management strategy. An organization-wide risk management strategy must include, at a minimum:

- Expression of the risk tolerance for the organization,
- Acceptable risk assessment methodologies,
- Risk mitigation strategies,
- A process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and
- Approaches for monitoring risk over time.

For details, see **NIST SP 800-37** and **NIST SP 800-39**.

### 545.3.1.10 Security Authorization Process (PM-10)
Effective Date: 10/10/2017

The CISO must develop, implement, and manage an Agency-wide security authorization

process, which tests the effectiveness of security controls and integrates with the Agency's risk management program. The authorization process requires approval by the CPO. At a minimum, an AO, SO, and ISSO must be designated for every major application, information system, and General Support System (including cloud-based systems). These roles serve as the primary contacts for all security matters related to those systems. For details, see **NIST SP 800-37** and the USAID Security Assessment and Authorization Procedure Guide (to obtain a copy of this document, please go to **https://pages.usaid.gov/M/CIO/security-assessment-and-authorization-saa**).

#### 545.3.1.11 Mission/Business Process Definition (PM-11)

Effective Date: 10/10/2017

The Agency, in coordination with M/CIO, must define and manage Mission/business processes, aligned with the Agency's Risk Management Framework, designed to counter threats to information, operations, personnel, and other Agency assets.

#### 545.3.1.12 Insider Threat Program (PM-12)

Effective Date: 10/10/2017

The USAID Office of Security (SEC), in collaboration with the CISO, must develop, implement, and oversee an Agency insider threat program to provide a central integration and analysis capability for Agency information. This program has been established to create controls to detect and prevent insider malicious activity and must ensure that USAID personnel understand and report potential threats. For details, see **ADS 569, Counterintelligence Program** and **EO 13587**.

#### 545.3.1.13 Information Security Workforce (PM-13)

Effective Date: 10/10/2017

The CISO, in coordination with M/CIO and the Office of Human Capital and Talent Management (HCTM), must establish an information security workforce program to institutionalize core information security capabilities. This includes defining knowledge and skills needed by the information security workforce, conducting training for them, and providing standards to evaluate their performance.

#### 545.3.1.14 Testing, Training and Monitoring (PM-14)

Effective Date: 10/10/2017

The CISO must develop, implement, and maintain an Agency-wide process to execute timely security testing, training, and monitoring; review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions; and review the results as part of ongoing risk assessments. The CISO must ensure that the organization performing testing has appropriate independence. For details, see **NIST SP 800-16**, **NIST SP 880-37**, **NIST SP 800-53A**, and **NIST SP 800-137**.

#### 545.3.1.15 Contacts with Security Groups and Organizations (PM-15)

Effective Date: 10/10/2017

The CISO and designees, must establish and maintain contact with selected external security groups. The purpose is to identify current cybersecurity related threats, tools, and techniques and train Agency staff to safeguard Agency assets and operations.

#### 545.3.1.16 Threat Awareness Program (PM-16)

Effective Date: 10/10/2017

The CISO must implement a threat awareness program that includes sharing threat information among general users, SOs, ISSOs, or their designees. Information sharing throughout the Agency on threat awareness mitigates risks, including Advanced Persistent Threat (APT), to Agency assets and operations. Sharing can consist of information on threat events, mitigations, and threat intelligence. Threat information sharing may be bilateral or multilateral. Some threat information may be highly sensitive requiring agreements and certain protections to be determined by the CISO.

### 545.3.2 Access Control (AC)

Effective Date: 10/10/2017

Access control limits who can interact with an information system. Proper access controls ensure only authorized staff gain access to information system resources.

#### 545.3.2.1 Access Control Policy and Procedures (AC-1)

Effective Date: 10/10/2017

The CISO must develop, disseminate, and review/update annually an access control policy. SOs must document, implement, and review/update annually access control procedures to comply with policy and to protect resources from unauthorized alteration, loss, unavailability, or disclosure.

#### 545.3.2.2 Account Management (AC-2)

Effective Date: 10/10/2017

Approvals by system ISSOs and SOs/SO designees are required for requests to create information system accounts and authorize access to the information system based on:

**a.** A valid access authorization,

**b.** Intended system usage, and

**c.** Other attributes as required by USAID or associated Missions/business functions.

SOs must:

**a.** Employ automated mechanisms, to the extent feasible, to support the management of information system accounts.

**b.** Configure the information system to automatically disable accounts after 90 days of inactivity. Users with disabled accounts must contact the M/CIO Service Desk to re-activate their accounts.

**c.** Assign an account manager (or group) for managing information system accounts.

**d.** Identify and select the following types of information system accounts to support organizational Missions/business functions:

**1)** Individual accounts,

**2)** System accounts,

**3)** Emergency accounts,

**4)** Developer/manufacturer/vendor accounts,

**5)** Temporary accounts, and

**6)** Service accounts.

**Note:** Any account identified as an emergency account or temporary account must be under strict CISO or CISO-designee control because emergency account and/or temporary account activation may bypass normal account authorization processes. If emergency and temporary accounts are authorized, the system must be configured to automatically disable the accounts after 30 days.

**e.** Establish conditions for group and role membership.

**f.** Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

**Note:** Group or shared accounts/passwords include anonymous, guest, temporary employees, administrative or service accounts, and accounts used in batch processing. The use of group accounts/passwords is limited to situations dictated by operational necessity or mission accomplishment and must be approved by the SO and documented in the System Security Plan (SSP). The ISSO or other designee must control, protect, and maintain such authenticators in accordance with this ADS chapter. Foreign Service Nationals (FSNs) may hold administrative positions that require elevated rights and privileges at Missions, to include critical threat environments.

**g.** Configure the information system to automatically audit account creation, modification, enabling, disabling, and removal actions, and notify as defined by SO.

**h.** Create audit logs whenever any of the following activities are requested to be performed by the system:

**1)** Granting, modifying, or revoking access rights, including adding a new user or group;

**2)** Changing user privilege levels;

**3)** Changing file permissions;

**4)** Changing database object permissions;

**5)** Changing firewall rules; and

**6)** Changing user passwords.

**i.** Monitor the use of information system accounts.

**j.** Review accounts for compliance with account management requirements semi-annually.

**k.** Create, enable, modify, disable, and remove information system accounts in accordance with **ADS 502, The USAID Records Management Program** and the **ISSO Handbook**.

SOs must not issue shared/group account credentials unless explicitly authorized by the CISO and M/CIO. SOs must only employ the use of emergency and temporary authorizations under strict CISO or CISO-designee control. If emergency and temporary accounts are authorized, the system must be configured to automatically disable the accounts after 72 hours. Accounts for users on extended absences must be temporarily suspended or disabled and the SO must establish a process to re-enable such accounts.

All SOs, Information Owners (IOs), and Bureaus must coordinate with ISSOs or M/CIO to establish a process to notify account managers when:

**a.** Accounts are no longer required,

**b.** Users are terminated or transferred, and

**c.** Individual information system usage or need-to-know changes occur.

#### 545.3.2.3 Access Enforcement (AC-3)

Effective Date: 10/10/2017

SOs must configure the information system to enforce access with approved credential methods for logical access to information and system resources in accordance with

**Homeland Security Presidential Directive-12 (HSPD-12)**, Identification and Authentication policies, and system-specific access policies.

### 545.3.2.4 Information Flow Enforcement (AC-4)

Effective Date: 10/10/2017

SOs must configure the information system to enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on interconnection security agreements (ISAs), memoranda of understanding (MOUs), memoranda of agreement (MOAs), and access control lists (ACLs) (see the **Policy and Quality Management (PQM) System Development Life Cycle (SDLC) site** for these and other SDLC templates).

### 545.3.2.5 Separation of Duties (AC-5)

Effective Date: 10/10/2017

SOs must separate critical information system functions among different individuals or groups; document separation of duties of individuals; and define information system access authorizations to support separation of duties. This is typically documented through a Separation of Duties matrix (for an example, see **https://www.usaid.gov/forms/aid-451-1**).

### 545.3.2.6 Least Privilege (AC-6)

Effective Date: 10/10/2017

SOs must:

**a.** Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks, in accordance with USAID's Missions and business functions.

**b.** Ensure that the Information System audits the execution of privileged functions.

**c.** Ensures the IS prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

**d.** Explicitly authorize access to:

**1)** System and network administration;

**2)** System account management;

**3)** Access authorization (i.e. permissions, privileges);

**4)** Audit log management; and

**5)** Setting intrusion detection parameters.

**e.** Assign separate identification and authorization credentials to users that require both privileged and non-privileged accounts.

**f.** Restrict privileged accounts on the information system to approved and authorized system administrators.

Privileged account holders must use only non-privileged credentials when performing non-privileged functions or roles. Staff, ISSOs, System Administrators (SAs), and other privileged users must not intentionally test, bypass, modify, or deactivate security controls implemented to protect USAID's information systems, unless authorized in writing by the CISO.

### 545.3.2.7 Unsuccessful Logon Attempts (AC-7)

Effective Date: 10/10/2017

SOs must configure the information system to enforce a limit of three consecutive, invalid logon attempts by a user within 30 minutes and automatically lock the account for a minimum of 30 minutes or until released by an administrator when the maximum number of unsuccessful logon attempts (three) is met.

SOs must configure smartphones and tablets to automatically wipe/purge information after 10 consecutive unsuccessful login attempts and must document and implement procedures to restore the secure baseline (see **545.3.20.2**, Mobile Devices).

### 545.3.2.8 System Notification (AC-8)

Effective Date: 10/10/2017

SOs must configure the information system to:

**a.** Display to users the system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, and states that:

**1)** Users are accessing a U.S. Government information system;

**2)** Information system usage may be monitored, recorded, and subject to audit;

**3)** Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

**4)** Use of the information system indicates consent to monitoring and recording.

**b.** Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the

information system.

**c.** For publicly accessible systems, SOs must display to users a system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, and includes a description of the authorized uses of the system (see **ADS 545sah, Warning Screen Messages Guidelines** for more information).

### 545.3.2.9 Session Lock and Termination (AC-11 and AC-12)

Effective Date: 10/10/2017

A session lock means that the system will automatically lock the computer after a predetermined period of inactive time. Session locks are typically configured at the operating system level, but may also be configured at the application level. Session locks are not an acceptable substitute for logging out of information systems at the end of the day or when prolonged absences are expected.

SOs must configure the information system to:

**a.** Initiate a session lock after 20 minutes of inactivity or when an end user manually initiates a session lock (for example, CTRL+ALT+DEL);

**b.** Ensure that end user devices lock after 20 minutes and application sessions terminate after 60 minutes of inactivity (see **545.3.17.7**, SC-10 for network session terminations);

**c.** Retain the session lock until the user re-authenticates;

**d.** Conceal, via the session lock, information previously visible on the display with a generic, publicly viewable image to obscure logon credentials; and

**e.** Automatically terminate a user session after a maximum of 60 minutes of inactivity.

### 545.3.2.10 Permitted Actions Without Identification or Authentication (AC-14)

Effective Date: 10/10/2017

SOs must:

**a.** Approve user actions that can be performed on the information system without identification or authentication consistent with organizational Missions/business functions; and

**b.** Document and provide supporting rationale regarding permitted actions in the information system security plan.

### 545.3.2.11 Remote Access (AC-17)

Remote access is used by USAID to allow access to organizational information systems (or processes acting on behalf of users) by communicating through external networks (i.e., the Internet).

Remote access to USAID information systems requires two-factor authentication. The mechanism must be approved by M/CIO and CISO. Currently, the only approved means are the HSPD-12 Personnel Identity Verification (PIV) or PIV-Alternative (PIV-A) cards and the hardware or software -based RSA SecurID tokens.

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 140-2, Security Requirements for Cryptographic Modules**.

Remote access to SBU, to include PII, must only be made using a virtual private network (VPN) or strong two-factor authentication using **FIPS 140-2** certified encryption to protect the information in transit as well as while at rest on a physical device. 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, as documented in the System Security Plan (SSP). The SSP and Risk Assessment must document any remote access of PII and must be approved by the Chief Privacy Officer prior to implementation. For more information regarding remote access of PII, see **ADS 508, The USAID Privacy Policy**. Remote Desktop Protocol (RDP) is not authorized for use for remote access.

To protect remote access connections, SOs must:

**a.** Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

**b.** Authorize remote access to the information system prior to allowing such connections.

**c.** Configure the information system to monitor and control remote access methods.

**d.** Implement cryptographic mechanisms, as described previously, to protect the confidentiality and integrity of remote access sessions based on the systems security categorization.

**e.** Route all remote accesses through managed access points (the number of managed access points is system specific).

**f.** Explicitly authorize the execution of privileged commands and access to security-relevant information via remote access only for all system administration except for security appliances, and document the rationale for such access in the security plan

for the information system.

Staff must not install or use remote control software unless approved by the M/CIO Change Control Board (CCB) and the CISO.

### 545.3.2.12 Wireless Access (AC-18)

Effective Date: 10/10/2017

SOs must:

**a.** Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access;

**b.** Authorize wireless access to the information system prior to allowing such connections;

**c.** Protect access to wireless communications via approved encryption mechanisms and user-based authentication;

**d.** For USAID Missions, select radio antennas and calibrate transmission power levels to reduce the probability that usable signals can be received outside of USAID-controlled boundaries; and

**e.** Develop guidance for discussing sensitive information on cellular phones. Under no circumstances must classified information be discussed on cellular phones.

See **545.3.20.2**, Mobile Devices, for additional information.

### 545.3.2.13 Access Control for Mobile Devices (AC-19)

Effective Date: 10/10/2017

The Agency must:

**a.** Prohibit the use of unclassified mobile devices in restricted spaces containing information systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and

**b.** Document and enforce restrictions on individuals permitted by the Authorizing Official to use unclassified mobile devices in restricted spaces containing information systems processing, storing, or transmitting classified information.

SOs must:

**1)** Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for USAID-controlled mobile devices;

**2)** Authorize the connection of mobile devices to organizational information systems;

and

**3)** Employ either full-device encryption or container encryption to protect the confidentiality and integrity of information on all Government Furnished Equipment (GFE) mobile devices and portable endpoint devices.

### 545.3.2.14 Use of External Information Systems (AC-20)

Effective Date: 10/10/2017

SOs must establish terms and conditions consistent with any trust relationships established with other organizations owning, operating, or maintaining external information systems. The terms and conditions must include provisions for allowing authorized individuals to access the information system from external information systems and process, store, or transmit USAID-controlled information using external information systems. This control recognizes that there are circumstances where members of the workforce using external information systems (i.e., contractors) need to access organizational information systems.

AOs must only authorize the use of external information systems to process, store, or transmit USAID-controlled information when USAID verifies the implementation of required security controls on the external system. For more information, see **USAID Security Assessment and Authorization (SA&A) Process**. This must be specified in the system security plan and in an approved information system connection agreement or similar agreements with the organizational entity hosting the external information system.

SOs must restrict the use of Agency-controlled portable storage devices by authorized individuals on external information systems.

Bring your own device (BYOD) wireless devices (WDs) are only authorized for use if explicitly approved in writing by CIO. Prior to the approval of BYOD, mobile security architecture must be developed, fully implemented, and assessed for effectiveness by the CISO. Additionally, M/CIO must create a policy documenting use and restrictions.

### 545.3.2.15 Information Sharing (AC-21)

Effective Date: 10/10/2017

AOs, in coordination with SOs, Information Owners, or Business Owners, must:

**a.** Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on sensitive information; and

**b.** Employ either automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

When it is determined that shared information is sensitive and requires additional security controls, an information sharing or similar agreement documenting security requirements

and responsibilities must be signed at a minimum by the sharing partner.

#### 545.3.2.16 Publicly Accessible Content (AC-22)
Effective Date: 10/10/2017

SOs must:

**a.** Designate individuals authorized to post information onto a publicly accessible information system;

**b.** Train authorized individuals to ensure that publicly accessible information does not contain non-public information;

**c.** Review the proposed content of information prior to posting it onto the publicly accessible information system to ensure that non-public information is not included; and

**d.** Review the content on the publicly accessible information system for non-public information at a minimum quarterly and remove such information, if discovered.

### 545.3.3 Awareness and Training (AT)
Effective Date: 10/10/2017

To protect the integrity, confidentiality, and availability of information and information assets, each person in the Agency must understand his/her roles and responsibilities and must be trained to perform them.

#### 545.3.3.1 Security Awareness and Training Policy and Procedures (AT-1)
Effective Date: 10/10/2017

The CISO must establish a formal security awareness and training policy and implementation procedures for users of USAID information systems. This policy must be documented, implemented, and reviewed/updated annually. The security awareness and training policy and program applies to any USAID staff with an account on a USAID information system. For more information, see the **USAID Security Training Policy, Standards, Guidelines, and Plan** (to obtain a copy of this document, email **ato@usaid.gov**).

#### 545.3.3.2 Security Awareness Training (AT-2)
Effective Date: 10/10/2017

The objectives of awareness training are to enhance awareness of the threats to, and vulnerabilities of, Agency information and information systems; and to encourage the use of good information security practices within USAID. There are several types of security awareness training.

**a. Initial Security and Privacy Awareness Training:** All USAID staff or others

working on behalf of USAID accessing USAID systems must receive initial training in security awareness and accepted security practices. Staff must complete security awareness training prior to being granted a user account. When access to an Information System is required by contract, the Contracting Officer's Representative (COR) must ensure that contractors complete the necessary training sessions.

**b. Annual Security and Privacy Awareness Training:** All USAID staff or others working on behalf of USAID or accessing USAID systems must receive annual refresher training in security awareness and accepted security practices. Staff must complete security awareness within the first year of being granted a user account. If the user fails to comply, the CISO will suspend system access. When access to an Information System is required by contract, the COR must ensure that contractors complete the necessary training sessions.

**c. Insider Threat Training:** Refer to **545.3.1.12**, Insider Threat Program (PM-12), for information on Insider Threat training. Refer to **ADS 569, Counterintelligence Program** or contact SEC for details on USAID's Insider Threat program.

**d. Awareness Training:** Awareness training must include, but is not limited to, wireless use and protection, including how to report a lost or stolen mobile device, how to maintain physical control of mobile devices or endpoints, and malicious code and malware protection.

### 545.3.3.3 Role-Based Security Training (AT-3)
Effective Date: 10/10/2017

Training provided to individuals assigned significant security responsibilities addresses general risk management and information security topics. SOs must identify personnel with significant security responsibilities and ensure that role-based training is completed, tracked, and records of such training are created and retained for review, in accordance with this ADS chapter.

All USAID staff and others working on behalf of USAID with significant security responsibilities (i.e., ISSOs and SAs) must receive role-based training specific to their security responsibilities upon assignment to the role, and refresher training yearly thereafter. When access to an Information System is required by contract, the COR must ensure that contractors complete the appropriate specialized training and refresher courses. Additional role-based training may be required as needed to address technology changes or patterns in threats and vulnerabilities in information systems.

### 545.3.3.4 Security Awareness Training Reporting and Non-Compliance (AT-4)
Effective Date: 10/10/2017

M/CIO/IA and SOs must track and maintain training records, and retain them in accordance with USAID record retention policies (see **ADS 502mab, Strategic Objective Document Disposition Schedule**), to include trainee name and position (if security role), date, and type of training received. SOs may maintain records of additional training

received. All evidence of training must be available upon the request of the Inspector General (IG), the CISO, and other governing entities.

All user accounts, including access to email, are disabled for users who do not comply with training requirements. Additionally, privileged/elevated rights are suspended for personnel identified as having significant security responsibilities who fail to comply with role-based training requirements.

In limited cases, extensions, not waivers or exemptions, may be granted in writing by the CISO; however, these cases must be justified, documented, and approved by the individual's supervisor.

### 545.3.4 Audit and Accountability (AU)

#### 545.3.4.1 Audit and Accountability Policy and Procedures (AU-1)
Effective Date: 10/10/2017

The policies and procedures of this chapter satisfy the requirements that the CISO must create an audit and accountability policy.

#### 545.3.4.2 Audit Events (AU-2)
Effective Date: 10/10/2017

The CISO must document both general and threat-specific logging guidance and the SO must document business specific logging guidance. The CISO and SO must review the set of required auditable security events annually and update as applicable. SOs must ensure that information systems are capable of and configured to log CISO defined and business specific auditable security events. For a full list of applicable events, see the **IA Audit and Accountability Guidance**.

#### 545.3.4.3 Content of Audit Records (AU-3)
Effective Date: 10/10/2017

SOs must ensure the Information System capability to correlate auditable events that are sufficient in detail to facilitate the reconstruction of security-relevant events if compromise or malfunction occurs or is suspected. All audit records must be reviewed as specified in the SSP for that respective system. For more information, see the **IA Audit and Accountability Guidance**.

M/CIO must provide a centralized management and configuration capability for audit content to be captured, stored, and monitored by information systems hosted on AIDNET. SOs must ensure that contracts or other agreements address the AU capability for systems not hosted on AIDNET.

#### 545.3.4.4 Audit Storage Capacity (AU-4) and Audit Record Retention (AU-11)
Effective Date: 10/10/2017

SOs must ensure that sufficient audit record storage capacity is allocated and that auditing is configured to reduce the likelihood of that capacity being exceeded. Audit records must be retained online for 90 days for immediate recall, and retained in offline storage for a minimum of 7 years.

Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. When storage capacity reaches 80 percent, the System Owner (SO) in coordination with the system maintenance provider must conduct an analysis and determination for increasing storage.

### 545.3.4.5 Response to Audit Processing Failures (AU-5)

Effective Date: 10/10/2017

SOs must configure the Information System to overwrite the oldest audit records in the event that storage capacity is reached, and to alert designated personnel in the event of an audit processing failure. SOs must define such designated personnel in the system security plan.

### 545.3.4.6 Audit Review, Analysis, and Reporting (AU-6)

Effective Date: 10/10/2017

SOs must ensure that audit records for Agency information systems are reviewed and analyzed at least weekly. This review and analysis must be documented as specified in the **IA Audit and Accountability Guidance** document. Unusual and suspicious activity or unexplained access attempts must be reported to the System or Mission ISSO, and a ticket opened with the M/CIO Service Desk at **cio-helpdesk@usaid.gov**."

M/CIO must:

**a.** Employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities; and

**b.** Provide a capability to analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

### 545.3.4.7 Audit Reduction and Report Generation (AU-7)

Effective Date: 10/10/2017

SOs must:

**a.** Ensure that the information system provides an audit reduction and report generation capability that supports an on-demand audit review, analysis, and reporting requirement and after-the-fact investigations of security incidents, and does not alter the original content or time ordering of audit records.

**b.** Ensure that the information system provides the capability to process audit records for events of interest based on criteria defined in the **IA Audit and Accountability Guidance** document.

### 545.3.4.8 Time Stamps (AU-8)
Effective Date: 10/10/2017

SOs must ensure that information systems use internal system clocks to generate time stamps for audit records. The time stamps generated by an Information System must include both date and time. The time may be expressed in either Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

The Information System (IS) must also synchronize internal IS clocks with an authoritative time source. M/CIO synchronizes internal IS clocks daily, via Network Time Protocol (NTP) to a USAID-approved time server, in accordance with domain controller policies.

### 545.3.4.9 Protection of Audit Information (AU-9)
Effective Date: 10/10/2017

SOs must protect their audit records and logs from unauthorized change, access, or destruction and must ensure that only explicitly authorized security professionals are given permissions and access to audit management functionality. These personnel must be designated in the SSP.

### 545.3.4.10 Audit Generation (AU-12)
Effective Date: 10/10/2017

SOs must ensure that information systems:

**a.** Provide an audit record generation capability for system components, auditable events, and content defined in the **IA Audit and Accountability Guidance** document; and

**b.** Allow the ISSO, or other designees, to select which auditable events must be audited by specific components of the information system.

## 545.3.5 Security Assessment and Authorization (SA&A)
Effective Date: 10/10/2017

When an information system is acquired or developed, a Security Assessment and Authorization (SA&A), is required in order for the system to obtain an Authority to Operate (ATO) (see definition in section **545.6**). An ATO must be received prior to deployment.

### 545.3.5.1 Security Assessment and Authorization Policy and Procedures (CA-1)
Effective Date: 10/10/2017

The CISO must:

**a.** Develop, disseminate, and at least annually, review/update a security assessment and authorization policy and procedures for implementation of the policy;

**b.** Specify automated tools, techniques, and methodologies used to assess, certify, and accredit USAID information systems;

**c.** Report and manage FISMA data;

**d.** Document and maintain Plan of Action and Milestones (POA&Ms); and

**e.** Assign common controls that may be shared or inherited by other systems and sites. The authorization package of those common controls must be shared with systems operating under the authoritative control of a higher system and each common control provider must assume responsibility for assigned controls by signing the authorization package and mitigating weaknesses identified through continuous monitoring.

#### 545.3.5.2 Security Assessments (CA-2)

Effective Date: 10/10/2017

Security assessors, including independent assessors or self-assessors, must develop a security assessment plan that describes the scope of the assessment, including:

**a.** Security controls and enhancements in scope;

**b.** Assessment procedures; and

**c.** Assessment environment, team, and roles and responsibilities.

SOs must assess the security controls in their information systems and their environment of operation at least annually to determine the extent to which the controls are:

**a.** Implemented correctly,

**b.** Operating as intended, and

**c.** Producing the desired outcome with respect to meeting established security requirements.

The assessment must produce a Security Assessment Report that documents the results of the assessment and must provide the results of the security control assessment to M/CIO/IA and the AO.

The CISO must determine the level of independence required for security assessments based on the system categorization, its business impact, and in special cases as

requested by USAID management. Systems with a security categorization of high or moderate must be assessed by an independent assessor at least every three years. A security assessment must be conducted for all new technology or systems that incorporate a new technology, such as social media, cloud computing, or wireless communication.

The Agency may accept the results of an external organizations' assessment of information systems categorized at the moderate or low level when performed by an independent assessor or Third Party Assessment Organization (3PAO) and only if explicitly approved by the CISO and AO. For guidance, see the **USAID Security Assessment and Authorization (SA&A) Process**.

#### 545.3.5.3 System Interconnections (CA-3) and Internal System Connections (CA-9)

Effective Date: 10/10/2017

M/CIO and SOs must authorize connections from USAID information systems to other information systems through the use of Interconnection Security Agreements (ISA). 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 or system. Interagency Agreements (IAs), Memoranda of Understanding (MOUs), and Service Level Agreements (SLAs) may also be used to document various aspects of interconnections. For additional information on MOUs, SLAs, ISAs, and MOAs, see **NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems**.

M/CIO must employ a deny-all, permit-by-exception policy with regards to allowing USAID systems to connect to external information systems.

SOs must:

**a.** Authorize all internal connections of USAID information systems;

**b.** Document the interface characteristics, security requirements, and the nature of the information communicated for each internal connection;

**c.** Review and update the ISA at least annually, and whenever there are changes that affect the terms of the agreement or the security of the information system. The ISA must be renewed every three years, or sooner if the conditions of the interconnection changes or if the ISA expiration date specifies it.

**Note:** Interconnections between USAID systems require an ISA whenever there is a difference in the security categorizations between the systems.

All interconnections must be coordinated through and approved by the CISO and M/CIO via Change Control Boards (CCBs) or other approval processes. Additionally, all interconnections must be fully documented in the SSP for USAID systems.

### 545.3.5.4 Plan of Actions and Milestones (CA-5)

Effective Date: 10/10/2017

When information system weaknesses or deficiencies are noted during assessments, audits, or other security related activities, SOs must develop Plans of Action and Milestones (POA&Ms) to document the planned remedial actions, and update the POA&Ms at least quarterly based on security monitoring activities.

SOs must ensure that information security requirements and POA&Ms are adequately funded, resourced, and documented in accordance with current OMB budgetary guidance. Detailed information for creating and managing POA&Ms appears in the **USAID POA&M Management Guide** and **Documenting Security Weaknesses in a POA&M** (to obtain a copy of these documents, please go to **https://pages.usaid.gov/M/CIO/security-assessment-and-authorization-saa** or send an email to **ato@usaid.gov**).

### 545.3.5.5 Security Authorizations (CA-6)

Effective Date: 10/10/2017

All USAID systems, including third-party systems and sites, must adhere to the standards defined in the **USAID Security Assessment and Authorization (SA&A) Process**. Type accreditations may also be granted as long as they meet M/CIO criteria as established in the SA&A Process document.

Each system must be appointed an SO, Information System Security Officer (ISSO), and an AO. These individuals must be appointed in writing in the authorization package. Each of these roles must be filled by different individuals in order to maintain appropriate separation of duties standards. Authorization/designation letters for ISSOs, AOs, and SOs are available on the **USAID Process and Quality Management (PQM) Web site**.

AOs must:

**a.** Authorize an information system for processing before it commences operations.

**b.** Update the security authorization at least every three years, or if there is a major change to the information system or environment that will affect the security of the system. A major change includes, but is not limited to:

**1)** Full version change for software or operating systems;

**2)** Physical environment change;

**3)** User community change;

**4)** New information types or categories; and

**5)** Other changes that might affect the security posture of the network, system, or information.

**c.** Authorize only systems that have been certified by the CISO and comply with M/CIO standards.

**d.** Accept risks for all systems for which an ATO is granted.

**e.** In coordination with the CISO, the AO may grant a restricted authority to operate (RATO) for systems that are undergoing development testing, piloting, or are in a prototype phase of development. However, such systems must not operate without an approved ATO or RATO. For additional guidance, see the **Security Requirements for Cloud-Based Production Prototypes and Proof of Concepts (PPPC) Projects** (to obtain a copy of this document, please send a request to the M/CIO Service Desk at **cio-helpdesk@usaid.gov**).

**Note:** An RATO is 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 six months and may grant one six-month extension. Systems under an RATO must not process sensitive information but may attach to system networks for testing.

**f.** Interim authority to operate (IATO) is not granted by the Agency and is not recognized by OMB.

SOs must:

**a.** Assign an impact level (low, moderate, or high) for each system based on assessment of security objectives (Confidentiality, Integrity, and Availability), in accordance with **Federal Information Processing Standards 199 (FIPS-199), Standards for Security Categorization of Federal Information and Information Systems**.

**b.** Employ **NIST SP 800-53, Rev. 4** (or current approved revision) controls based on a tailored set of controls specific to the system and security objective and approved by the CISO. SOs must work with the common control providers to tailor the security controls specific to the system and the security objective.

M/CIO may revoke an ATO for any USAID system if it is determined that the system does not comply with USAID standards or presents an unacceptable risk to the Agency. For more information, see the **USAID Security Assessment and Authorization (SA&A) Process**.

### 545.3.5.6 Continuous Monitoring (CA-7)

Effective Date: 10/10/2017

M/CIO must:

**a.** Develop a continuous monitoring strategy (see the **Information Systems Continuous Monitoring (ISCM) Strategy** (to obtain a copy of this document, please send an email to **ato@usaid.gov**).

**b.** Implement a continuous monitoring program that includes:

**1)** Establishment of security metrics to be monitored;

**2)** Methods by which the metrics will be monitored, assessed, and reported; and

**3)** Frequency of metrics.

**c.** Establish and maintain either independent assessors or independent assessment teams, based on the system security categorization and business impact, to monitor the security controls in the information system on an ongoing basis.

SOs must perform and document continuous monitoring activities in accordance with the **Information Systems Continuous Monitoring (ISCM) Strategy** (to obtain a copy of this document, please send an email to **ato@usaid.gov**).

### 545.3.6 Configuration Management (CM)
Effective Date: 10/10/2017

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 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 as well as subsequent approved changes.

#### 545.3.6.1 Configuration Management Policies and Procedures (CM-1)
Effective Date: 10/10/2017

The CISO must develop, document, disseminate, review annually and update as required, a configuration management policy.

SOs must:

**a.** Document, implement, and enforce procedures within the System Security Plan

(SSP) to comply with that policy and associated controls; and

**b.** When considering proposed changes, ensure that CM processes for their systems reflect the results of a security impact analysis.

### 545.3.6.2 Baseline Configuration (CM-2)

Effective Date: 10/10/2017

SOs must:

**a.** Develop, document, and maintain a current baseline of the information system. The baseline must be consistent with CISO secure baselines;

**b.** Review baselines annually and update as required or when major changes to the information system warrant;

**c.** Retain two previous baselines to support rollback;

**d.** Coordinate with the CISO to establish specific baselines for all network devices and endpoints, including mobile computing devices, for use in high-risk areas;

**e.** Ensure that baselines are applied to mobile GFE computing devices prior to such travel;

**f.** Ensure that the SSP or appendices specify the configurations required for such high risk travel;

**g.** For mobile devices, ensure that processes for securing the devices are documented and implemented and that the standard baseline configurations are applied upon the user's return; and

**h.** Alternatively, may issue mobile devices designated specifically and only for such travel. Such devices must be sanitized in accordance with CISO approved methods upon return from travel.

**Note:** Due to its rapid response requirements, the Office of U.S. Foreign Disaster Assistance (OFDA) maintains and follows its own comprehensive set of security controls for travel with wireless devices (WDs), which may vary from standard USAID policy but is in compliance with applicable FISMA and NIST guidelines. These deviations must be documented in the SSP and SAR.

### 545.3.6.3 Configuration Change Control (CM-3)

Effective Date: 10/10/2017

M/CIO must:

**a.** Determine the types of changes to the information system that are configuration-

controlled, review, approve/disapprove with explicit consideration for security impact, document change decisions, and retain change records for at least three years;

**b.** Audit and review changes to the system; and

**c.** Establish a process that coordinates and provides oversight for configuration/change management activities through a change control board that convenes at least monthly. A security representative must be a member of the change control board.

SOs must test, validate, and document changes to the information system before implementing the changes on the operational system.

#### 545.3.6.4 Security Impact Analysis (CM-4)

Effective Date: 10/10/2017

M/CIO must analyze proposed changes to the information system to determine potential security impacts prior to change implementation, and make recommendations based on that analysis.

#### 545.3.6.5 Access Restrictions for Change (CM-5)

Effective Date: 10/10/2017

SOs must define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system, including upgrades and modifications. Changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems.

#### 545.3.6.6 Configuration Settings (CM-6)

Effective Date: 10/10/2017

The CISO must establish and document baseline configuration settings for various IT equipment (see the **M/CIO Security Baselines Web page** for baseline configuration documents).

SOs must:

**a.** Implement the configuration settings;

**b.** Identify, document, and approve any deviations from established configuration settings for operating systems, databases, management systems, hardware, firmware and other technology as required by the CISO based on Mission or business specific operational requirements;

**c.** Monitor and control changes to the configuration settings in accordance with this ADS chapter, M/CIO change control procedures, and the system's Configuration Management Plan; and

**d.** Procure and allow use of only GFE wireless and mobile devices that allow secure configurations as defined by the CISO and the security architecture, that prohibit alterations, and that can be centrally managed by M/CIO.

### 545.3.6.7 Least Functionality (CM-7)

Effective Date: 10/10/2017

SOs must:

**a.** Ensure that systems are configured to provide only business essential capabilities and that the relevant M/CIO-approved ports, protocols, and/or services are documented in the SSP and reflected in the system baseline configurations;

**b.** Review the information system, at least quarterly, to identify unnecessary and/or non-secure functions, ports, protocols, and services;

**c.** Disable all unapproved ports, protocols, and services within the information system that are deemed to be unnecessary and/or non-secure;

**d.** Ensure that information systems prevent program execution in accordance with **ADS 545mbd, Rules Of Behavior for Users**;

**e.** Identify software programs authorized to execute on the information system by referencing the USAID Software Portfolio; and

**f.** Employ a deny-all, permit by exception policy to allow the execution of authorized software programs on the information system.

M/CIO must review and update the list of authorized software programs at a minimum monthly.

### 545.3.6.8 Information System Component Inventory (CM-8)

Effective Date: 10/10/2017

SOs must:

**a.** Maintain a list of all systems, hardware, and software in the information system's boundary, to include but not limited to cloud, social media, and mobile devices.

**b.** Verify that the system/components are not duplicated in another information system's inventory.

**c.** Ensure that all hardware and applications are captured in the accreditation boundary of an information SSP.

**d.** Ensure the inventory is at the level of granularity deemed necessary for tracking and

reporting. The inventory specifications include:

**1)** Vendor/manufacturer name and component name;

**2)** Hardware model number, item description, and serial number;

**3)** Hardware configuration (i.e. two Intel xxxxxx quad processors and one gigabyte of RAM);

**4)** Software version number and description;

**5)** Software license information including seats, number of licenses, etc. as applicable; and

**6)** Physical location of hardware.

SOs must ensure that the inventory is updated as an integral part of the change management process and at a minimum annually. M/CIO and/or SOs must employ automated mechanisms on a continuous basis to detect the presence of unauthorized hardware, software, and firmware components throughout the Agency.

When unauthorized components are detected, SOs must notify the M/CIO Service Desk and disable network access by such components.

### 545.3.6.9 Configuration Management Plan (CM-9)

Effective Date: 10/10/2017

SOs must:

**a.** Develop, document, and implement a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures;

**b.** Establish a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

**c.** Define the configuration items for the information system and place the configuration items under configuration management; and

**d.** Protect the configuration management plan from unauthorized disclosure and modification.

### 545.3.6.10 Software Usage Restrictions (CM-10)

Effective Date: 10/10/2017

SOs must:

**a.** Use software and associated documentation in accordance with contract agreements and copyright laws;

**b.** Employ tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and

**c.** Control and document the use of peer-to-peer file sharing technology, if it is explicitly authorized, to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

The CISO must approve the use of freeware, shareware, file-sharing, and open source software. Approval is based on an assessment of risk and the total life cycle cost (see **OMB Memo M-04-16, Software Acquisition** for acquisition guidance regarding this type of software). For guidance on cloud-related service contracts, see **Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service**.

#### 545.3.6.11 User Installed Software (CM-11)
Effective Date: 10/10/2017

Members of the workforce are not authorized to install software, in accordance with the **ADS 545mbd Rules of Behavior for Users**. Staff requiring installation of software must contact the M/CIO Service Desk.

SOs must:

**a.** Establish software configuration and installation procedures that align to this ADS chapter to govern the installation of software by users;

**b.** Enforce software installation policies through role-based rights management; and

**c.** Monitor policy compliance at least monthly.

### 545.3.7 Contingency Planning (CP)
Effective Date: 10/10/2017

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.

#### 545.3.7.1 Contingency Planning Policy and Procedures (CP-1)
Effective Date: 10/10/2017

The CISO must develop, document, review annually, update as required, and disseminate to the USAID staff a contingency planning policy. SOs must document, implement, and enforce procedures to comply with contingency planning policies and associated contingency plan (CP) control requirements.

### 545.3.7.2 Contingency Plan (CP-2)

Effective Date: 10/10/2017

SOs must:

**a.** Develop a contingency plan for the information system that:

**1)** Identifies incident handling activities;

**2)** Identifies essential missions and business functions and associated contingency requirements;

**3)** Provides recovery objectives, restoration priorities, and metrics;

**4)** Addresses contingency roles, responsibilities, and assigned individuals with contact information;

**5)** Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

**6)** Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;

**7)** Plans for the resumption of essential missions and business functions consistent with time frames identified in the system's Business Impact Analysis (BIA); and

**8)** Identifies critical information system assets supporting essential missions and business functions.

**b.** Coordinate CP development with organizational elements responsible for related plans, including Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plans, and Occupant Emergency Plans.

**c.** Review the CP annually.

**d.** Update the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing.

**e.** Obtain approvals for the CP and subsequent updates from the AO and the business owner(s) (if identified).

**f.** Communicate CP changes to business owner(s) and key contingency personnel.

**g.** Distribute copies of the CP to the business owner(s) and key contingency personnel, identified by name or by role in the plan.

**h.** Protect the CP from unauthorized disclosure and modification.

### 545.3.7.3 Contingency Training (CP-3)
Effective Date: 10/10/2017

SOs must provide contingency training to users with assigned CP roles and responsibilities within 90 days of assuming a contingency role/responsibility, and annually.

### 545.3.7.4 Contingency Plan Testing (CP-4)
Effective Date: 10/10/2017

SOs must:

**a.** Ensure that testing is performed in accordance with the availability security objective;

**b.** Test CPs for their information system(s) annually;

**c.** Coordinate CP testing or exercises as appropriate with organizations with related plans for systems with moderate and high availability, per the **FIPS 199** security categorization; and

**d.** While CP tests may be simulated, tabletop, or actual, SOs must ensure that an actual test of at least one component is completed at least every three years.

### 545.3.7.5 Alternate Storage Site (CP-6)
Effective Date: 10/10/2017

SOs must:

**a.** Establish an alternate storage site that:

**1)** Provides information security safeguards equivalent to those of the primary site, including necessary agreements to permit the storage and recovery of information system backup information.

**2)** Is geographically separated from the primary storage site, so as not to be susceptible to the same hazards.

**Note:** The AO or SO may determine the level of separation that is sufficient based on the risk analysis.

**b.** In collaboration with the service provider, create Alternate Storage Agreements. The agreements must include, but are not limited to, the following:

**1)** City and state of alternate storage site, and distance from primary facility;

**2)** Whether the alternate storage site is owned by the organization or is a third-party storage provider;

**3)** Name and points of contact for the alternate storage site;

**4)** Delivery schedule and procedures for packaging media to go to alternate storage site;

**5)** Procedures for retrieving media from the alternate storage site;

**6)** Names and contact information for those persons authorized to retrieve media;

**7)** Any potential accessibility problems to the alternate storage site in the event of a widespread disruption or disaster;

**8)** Mitigation steps to access alternate storage site in the event of a widespread disruption or disaster;

**9)** Types of data located at alternate storage site, including databases, application software, operating systems, and other critical information system software;

**10)** If electronic accessibility to the alternate storage site is disrupted, plans for physical access to retrieve backup information; and

**11)** Other information as deemed appropriate by the system owner.

### 545.3.7.6 Alternate Processing Site (CP-7)

Effective Date: 10/10/2017

SOs must:

**a.** Establish an alternate processing site including necessary agreements to permit the transfer and resumption of operations defined by the system or business owner for essential Missions/business functions. The time periods for transfer and resumption of operations must be consistent with recovery time objectives (RTO) and recovery point objectives (RPO) documented in the BIA;

**b.** Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the time periods consistent with RTO and RPO documented in the

BIA for transfer/resumption;

**c.** Ensure that the alternate processing site provides information security safeguards equivalent to those of the primary site;

**d.** Ensure that the alternate processing site is sufficiently separated from the primary processing site to reduce susceptibility to the same threats;

**e.** Ensure that agreements or contracts identify and address potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions; and

**f.** Ensure that agreements include priority-of-service provisions in accordance with availability requirements.

### 545.3.7.7 Telecommunications Services (CP-8)

Effective Date: 10/10/2017

SOs must establish or ensure alternate telecommunications services, including necessary agreements to permit resumption of services identified by the SO for essential Mission and business functions, consistent with availability requirements identified in the BIA. At a minimum, the agreements must contain priority-of-service provisions for national security emergency preparedness to reduce the likelihood of single points of failure.

If this capability is not provided by USAID M/CIO, SOs must ensure that agreements or contracts address alternate telecommunications service requirements.

### 545.3.7.8 Information System Backup (CP-9)

Effective Date: 10/10/2017

SOs must:

**a.** Conduct or require backups of the following information:

- System and security-related documentation,
- User-level, and
- System-level.

**b.** Ensure the documentation/information is backed up at a frequency consistent with the RTO and RPO that are identified in the system BIA.

**c.** Protect the confidentiality, integrity, and availability of backup information at storage locations by using approved encryption mechanisms consistent with the policies in this document, or by other CISO approved manual processes.

**d.** Ensure backups are tested annually, at a minimum.

**e.** Retain test results for a minimum of one year.

### 545.3.7.9 Information Recovery and Reconstitution (CP-10)
Effective Date: 10/10/2017

SOs must provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure and must implement transaction recovery mechanisms for systems that are transaction-based.

### 545.3.8 Identification and Authorization (IA)
Effective Date: 10/10/2017

SOs must control and limit all user access through positive user identification and authentication mechanisms that support at a minimum access control, least privilege, and system integrity.

Applicable controls include the **NIST SP 800-53** IA control family as selected for the highest risk level of the applicable system or the highest risk level associated with any supported system for general support systems. Generally, identification is an assertion by the user of a unique identity (i.e. a username); authentication is proof of that identity (i.e., a password).

### 545.3.8.1 Identification and Authorization Policy and Procedures (IA-1)
Effective Date: 10/10/2017

The CISO must develop, document, and disseminate to USAID staff an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The CISO must review the policy annually and update said policy as required.

SOs must document, implement, and enforce procedures to comply with identification and authentication policy and associated identification and authentication controls. SOs must review the procedures annually and then as required.

### 545.3.8.2 Identification and Authentication (Organizational Users) (IA-2)
Effective Date: 10/10/2017

Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, Direct-Hires, PSCs). SOs must:

**a.** Ensure that the information system uniquely identifies and authenticates organizational users or processes acting on behalf of organizational users;

**b.** Implement or employ multifactor authentication for network access for all accounts, and multifactor authentication for local access for privileged accounts;

**c.** Implement replay-resistant authentication mechanisms for network access to privileged accounts. Replay-resistant techniques include, for example, protocols that use one-time random numbers or challenges, such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators;

**d.** Implement multifactor authentication for remote access for privileged and non-privileged accounts such that one of the factors is provided by a device separated from the system gaining access and the device meets **NIST 800-157**. Hard tokens and soft tokens can meet this requirement; and

**e.** Configure the information system to accept and electronically verify Personal Identity Verification (PIV) or PIV-A credentials or **NIST SP 800-63-2** Level of Assurance 4 (LOA-4) credentials.

Any multifactor authentication requires Agency-controlled certificates or hardware/ software tokens issued directly to each authorized user.

#### 545.3.8.3 Device Identification and Authentication (IA-3)
Effective Date: 10/10/2017

SOs must ensure that the information system uniquely identifies and authenticates all endpoints and mobile devices before establishing a remote or network connection.

#### 545.3.8.4 Identifier Management (IA-4)
Effective Date: 10/10/2017

SOs must manage information system identifiers by:

**a.** Receiving authorization from AMS Officers, the user's Direct-Hire Supervisor, the COR, or other Direct-Hire designees to assign an individual, group, role, or device identifier;

**b.** Selecting an identifier that identifies an individual, group, role, or device;

**c.** Assigning the identifier to the intended individual, group, role, or device;

**d.** Preventing reuse of identifiers for 10 years; and

**e.** Disabling the identifier after 90 days.

#### 545.3.8.5 Authenticator Management (IA-5)
Effective Date: 10/10/2017

SOs must conform to the minimum requirements described below; however, SOs must determine whether higher level restrictions and conditions beyond these minimum requirements should be established in light of the risks involved with respect to the

particular system. SOs must assure that the final restrictions and conditions are documented in the SSP.

SOs must manage information system authenticators by:

**a.** Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

**b.** Establishing initial authenticator content for authenticators defined by the organization;

**c.** Ensuring that authenticators have sufficient strength for their intended use;

**d.** Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

**e.** Changing default content of authenticators prior to information system installation;

**f.** Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

**g.** Changing/refreshing authenticators at a minimum of every 90 days;

**h.** Protecting authenticator content from unauthorized disclosure and modification;

**i.** Requiring individuals to take specific security safeguards to protect authenticators and implementing mechanisms to facilitate such safeguards; and

**j.** Changing authenticators for group/role accounts when membership to those accounts changes.

SOs must ensure the information system does the following regarding passphrases and password-based authentication:

**1)** Enforces minimum password complexity of at least 12 characters, mix of at least one character from each of three of the following four character types: upper-case letters, lower-case letters, numbers, and special characters;

**2)** Enforces at least the following number of changed characters when new passwords are created: four characters must be changed;

**3)** Stores and transmits only encrypted passwords;

**4)** Enforces password minimum and maximum lifetime restrictions, with no minimum lifetime and a maximum lifetime of 60 days;

**5)** Prohibits password reuse for 24 generations;

**6)** Allows the use of a temporary password for system logons only with an immediate change upon first-time logon to a new password; and

**7)** Prevents embedding passwords in scripts or source code.

SOs must ensure the information system does the following for PKI-based authentication (see **545.3.8.7, Cryptographic Module Authentication (IA-7)**):

- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
- Enforces authorized access to the corresponding private key;
- Maps the authenticated identity to the account of the individual or group;
- Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network; and
- Ensures that PKI-based authenticators are controlled, protected, and maintained in accordance with ADS policy.

Biometric devices use behavioral or physiological characteristics (such as vein mapping, retina scan, iris scan, or fingerprints) to determine or verify a user's identity. These controls provide access to the network, systems, email and other areas, and require careful management.

The CISO must approve all biometric authentication methods. When biometric authentication methods are in use, authentication procedures must be developed and implemented. Staff must receive training in the secure use of biometric devices. Biometrics that are captured or transmitted by the Agency must be protected with the use of approved encryption mechanisms. When biometrics is used for authentication, a PIN or passcode must also be used for authentication. All PINs and passcodes must be a minimum of six characters.

USAID staff must not share any authenticators such as PINs, passphrases, passwords, or passcodes that are not approved for group use.

M/CIO must require the registration process to receive token or PKI-based authenticators be conducted in person by the USAID Enrollment Office or by a trusted third party (i.e. Mission Staff) if approved by M/CIO and the CISO.

SOs must ensure that token-based authentication employs mechanisms that satisfy

requirements described in **NIST SP 800-63**; **NIST SP 800-157**; **HSPD-12**; and USAID encryption standards.

USAID encryption standards are as follows: Systems requiring encryption must use 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. SOs must develop and maintain encryption plans for sensitive information systems requiring encryption. 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.

#### 545.3.8.6 Authenticator Feedback (IA-6)
Effective Date: 10/10/2017

SOs must configure the information system to obscure authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

#### 545.3.8.7 Cryptographic Module Authentication (IA-7)
Effective Date: 10/10/2017

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

SOs must implement, in the information system, mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication, including **FIPS 140-2** and **FIPS 197**.

Systems requiring encryption must provide algorithms with at least 256-bit encryption validated under Type 2 or Type 1 encryption.

#### 545.3.8.8 Identification and Authentication (Non-Organizational Users) (IA-8)
Effective Date: 10/10/2017

Non-organizational users are information system users other than the organizational users covered by IA-2 (in **545.3.8.2, Identification and Authentication (Organizational Users) (IA-2)**). SOs must:

**a.** Ensure that the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

**b.** Ensure that the information system:

**1)** Accepts and electronically verifies Personal Identity Verification (PIV)

credentials from other federal agencies;

**2)** Accepts only Federal Identity, Credentialing, and Access Management (FICAM)-approved third-party credentials;

**3)** Employs only FICAM-approved information system components in enterprise level information systems to accept third-party credentials; and

**4)** Confirms to FICAM-issued profiles.

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 FICAM initiative, see **Idmanagement.gov**.

### 545.3.9 Incident Response (IR)
Effective Date: 10/10/2017

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 than ever before. An Incident Response (IR) capability is therefore necessary for quickly detecting incidents, minimizing loss and destruction, mitigating the exploited weaknesses, and restoring computing services.

#### 545.3.9.1 Incident Response Policy and Procedures (IR-1)
Effective Date: 10/10/2017

The CISO must establish, disseminate, and review/update annually, a documented incident response policy.

SOs must coordinate with the CISO to establish and implement procedures to facilitate the incident response policy and associated incident response controls. This documentation must be reviewed/updated at a minimum annually.

More information on the USAID Continuous Incident Response Capability procedures can be found in the **Incident Response Program Concept of Operations (CONOPS)** document (to obtain a copy of this document, please send a request to the M/CIO Service Desk at **cio-helpdesk@usaid.gov**).

#### 545.3.9.2 Incident Response Training (IR-2)
Effective Date: 10/10/2017

As part of the continuous incident response capability, the CISO must train staff with incident response roles and responsibilities within 30 calendar days of assignment, and provide refresher training annually.

### 545.3.9.3 Incident Response Testing (IR-3)
Effective Date: 10/10/2017

In coordination with CISO, SOs must test annually the incident response capability with table top exercises and using documented results to validate the incident response effectiveness.

### 545.3.9.4 Incident Handling (IR-4)/Incident Monitoring (IR-5)
Effective Date: 10/10/2017

The CISO must implement an incident handling procedure to include an automated capability to assist in tracking of security incidents and in collection and analysis of incident information.

The automated capability for incident handling and monitoring must:

**a.** Include preparation, detection and analysis, containment, eradication, and recovery.

**b.** 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.

**c.** Implement the resulting changes accordingly. Activities include the following:

**1)** Track and document information system security incidents;

**2)** Require staff to report suspected security incidents to the organizational incident response capability as soon as discovered and report security incident information to designated authorities; and

**3)** SOs and ISSOs must document information system-specific service desk and incident handling procedures in their information system's System Security Plan (SSP).

For more information, refer to the system incident response procedures, available from the System or Mission ISSO.

### 545.3.9.5 Incident Reporting (IR-6)/Incident Assistance (IR-7)
Effective Date: 10/10/2017

The CIO must provide incident response support resources, integral to the Agency incident response capability, that offer advice and assistance to users of the information system for the handling and reporting of security incidents.

Staff must report security incidents as soon as discovered to the M/CIO Service Desk at **cio-helpdesk@usaid.gov**.

The organization employs automated mechanisms to increase the availability of incident response-related information and support. See IR-5 for more information on automated incident reporting requirements (see **ADS 508, The USAID Privacy Policy** for information on Privacy Incident Reporting).

If users know or suspect that their mobile device (MD) has been compromised, they must immediately turn off the MD and deliver it to the System or Mission ISSO, who then must immediately report the incident to the M/CIO Service Desk at **cio-helpdesk@usaid.gov**. The M/CIO Service Desk will provide further guidance. The user must not allow the compromised/possibly compromised MD to connect to any networks (wireless or wired) or GFE.

### 545.3.9.6 Incident Response Plan (IR-8)

Effective Date: 10/10/2017

The CISO must:

**a.** Provide the Agency with a roadmap/plan for implementing the Agency's incident response capability, distribute copies of the roadmap to SOs and ISSOs as required, and review the roadmap annually;

**b.** Describe the structure and organization of the incident response capability;

**c.** Provide a high-level approach for how the incident response capability fits into the overall organization;

**d.** Meet the unique requirements of the organization, which relate to mission, size, structure, and functions;

**e.** Define reportable incidents;

**f.** Provide metrics for measuring the incident response capability within the organization;

**g.** Define the resources and management support needed to effectively maintain and mature an incident response capability; and

**h.** Review and approve incident response plan.

SOs must:

**a.** Develop an incident response plan for implementing the incident response capability and review the plan annually. Disaster Recovery and Incident Response plans must include provisions for public/internal notifications within 30 days of detection/discovery and specify metrics and procedures for tracking public/internal notifications;

**b.** 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;

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

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

**e.** Protect the plan from unauthorized disclosure and modification.

### 545.3.10 Maintenance (MA)

Effective Date: 10/10/2017

System maintenance involves the repair and upkeep of systems or devices. Keeping systems and devices running may also require outside personnel to access the system or related information. All management personnel must take steps to ensure that maintenance activities are conducted in a manner that maintains security.

#### 545.3.10.1 System Maintenance Policy and Procedures (MA-1)

Effective Date: 10/10/2017

The CISO must develop, document, disseminate, review annually, and update as required, a systems maintenance policy. SOs must document and enforce procedures to implement the maintenance policy and associated maintenance security controls. The procedures and applicable controls must be documented in the SSP.

#### 545.3.10.2 Controlled Maintenance (MA-2)

Effective Date: 10/10/2017

SOs must:

**a.** Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications or organizational requirements;

**b.** Approve and monitor all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location;

**c.** Explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

**d.** Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

**e.** Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions;

**f.** Disable maintenance ports during normal operations; and

**g.** Include the following information in organizational maintenance records:

- System name,
- Components/serial number affected,
- Description of maintenance,
- Date of maintenance,
- Name of person performing maintenance, and
- Parts replaced.

### 545.3.10.3 Maintenance Tools (MA-3)

Effective Date: 10/10/2017

SOs must:

**a.** Approve, control, monitor the use of, and maintain on an ongoing basis, information system maintenance tools.

**b.** Establish procedures, referenced or included in the SSP, to:

**1)** Ensure that maintenance tools carried into the facility are checked for improper or unauthorized modifications before use on any USAID system; and

**2)** Ensure that media containing diagnostic and test programs are checked for malicious code before use on any USAID system.

### 545.3.10.4 Non-Local Maintenance (MA-4)

Effective Date: 10/10/2017

SOs must:

**a.** Explicitly authorize, in writing, only cleared personnel to perform non-local maintenance and diagnostics; and

**b.** If non-local maintenance is allowed, the policies and procedures for non-local maintenance and diagnostic connections must be clearly documented in the SSP.

### 545.3.10.5 Maintenance Personnel (MA-5)

Effective Date: 10/10/2017

SOs must:

**a.** Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

**b.** Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations; and

**c.** Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

#### 545.3.10.6 Timely Maintenance (MA-6)

Effective Date: 10/10/2017

The SOs must obtain maintenance support and/or spare parts for system components defined in the SSP within 24 hours of failure or as determined by the Business Impact Analysis (BIA).

### 545.3.11 Media Protection (MP)

#### 545.3.11.1 Media Protection Policy and Procedures (MP-1)

Effective Date: 10/10/2017

The CISO must develop, document, review annually, update as required, and disseminate to the USAID staff a media protection policy.

SOs must document, implement, follow, and enforce procedures to comply with media protection policies and associated media protection controls. The procedures must include provisions for protecting paper and electronic outputs that come from systems containing sensitive information.

#### 545.3.11.2 Media Access (MP-2)

Effective Date: 10/10/2017

SOs or information owners (IOs) must restrict access to all media, both digital and non-digital, containing sensitive information to only those personnel with a need to know.

Staff and others working on behalf of USAID must not:

- Use non-government issued removable media (USB drives, in particular);
- Connect non-government issued removable media to USAID equipment or networks; and

- Use non-government issued removable media to store USAID sensitive information.

### 545.3.11.3 Media Marking (MP-3)
Effective Date: 10/10/2017

SOs must mark information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and explicitly exempt media containing only non-sensitive or publicly releasable data from marking as long as the media remain within USAID control.

Media determined by SOs or IOs to contain sensitive information must be appropriately marked, in accordance with **12 FAM 540**.

### 545.3.11.4 Media Storage (MP-4)
Effective Date: 10/10/2017

SOs and IOs must:

**a.** Physically control and securely store digital or non-digital media containing sensitive information within USAID controlled areas or in a locked office, room, desk, file cabinet, locked tape device, or other storage prohibiting access by unauthorized person; and

**b.** Protect information system media until the media is destroyed or sanitized using CISO approved equipment, techniques, and procedures.

### 545.3.11.5 Portable Media Transport (MP-5)
Effective Date: 10/10/2017

All staff must:

**a.** Control the transport of information system media containing sensitive data, outside of controlled areas and restrict pickup, receipt, transfer, and delivery to authorized staff;

**b.** Maintain accountability for information system media during transport outside of controlled areas;

**c.** Follow the procedures established by **12 FAM 540** and **12 FAM 660** for the transportation or mailing of sensitive media. SOs must reference these guidelines or establish procedures aligned to these guidelines in the system SSP; and

**d.** Ensure that sensitive data is encrypted using **FIPS 140-2** compliant mechanisms during transport out of USAID controlled areas.

### 545.3.11.6 Media Sanitization (MP-6)

Effective Date: 10/10/2017

The CISO must define the approved methods for sanitization in accordance with applicable federal standards (**NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization**) and ensure the methods are commensurate with various security categorization levels of the information.

SOs must sanitize any information system storage media containing sensitive information, prior to disposal, release out of organizational control, or release for reuse using CISO-approved methods in accordance with applicable federal and organizational standards and policies.

SOs must employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information outlined in **NIST SP 800-88 Rev. 1**.

SOs must provide the capability to purge/wipe information from mobile devices when the device is reported as lost.

If degaussing equipment is employed as a sanitization method, SOs must periodically test the equipment to verify that it functions properly.

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

SOs must periodically test degaussing equipment to verify that the equipment is functioning properly.

#### 545.3.11.7 Media Use (MP-7)

Effective Date: 10/10/2017

M/CIO restricts the use of removable storage media, such as USB thumb drives, flash drives, and all mobile devices on all USAID information systems. Automated capabilities must be used to detect the presence of unauthorized USB devices on all USAID networks/information systems.

SOs must prohibit the use of portable storage devices within information systems when such devices have no identifiable owner.

### 545.3.12 Physical and Environmental Protection (PE)

#### 545.3.12.1 Physical and Environmental Protection Policy and Procedures (PE-1)

Effective Date: 10/10/2017

The Agency must develop, disseminate, review annually, and update as required documented physical and environmental protection policies and procedures.
SOs must establish, document, implement and enforce system specific procedures to

facilitate the implementation of associated physical and environmental protection physical and environmental protection controls.

Facilities processing, transmitting, or storing sensitive information must incorporate physical protection measures based on the level of acceptable risk.

For more information regarding USAID Physical Security Programs, see **ADS 565, Physical Security Programs (Domestic)**, **ADS Chapter 562, Physical Security Programs (Overseas)**, and **ADS 519, Building Support Services in USAID/Washington**.

### 545.3.12.2 Physical Access Authorizations (PE-2)
Effective Date: 10/10/2017

The Agency must:

**a.** Develop and keep current a list of staff and personnel with authorized access to the facility where an information system resides (except for those areas within the facility officially designated as publicly accessible);

**b.** Review and approve the access list and authorization credentials within at least annually;

**c.** Remove staff from the access list when they no longer require access to the facility; and

**d.** Issue authorization credentials for facility access.

For more information, see the **Office of Security (SEC) Common Controls Catalog** (to obtain a copy of this document, please send an email to **ato@usaid.gov**).

### 545.3.12.3 Physical Access Control (PE-3) and Visitor Access Records (PE-8)
Effective Date: 10/10/2017

The Agency must:

**a.** Enforce physical access authorizations at entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access, and controlling ingress/egress to the facility using physical access control or guards;

**b.** Maintain physical access audit logs and access records for entry/exit points to the facilities;

**c.** Provide inspections via manual or automated processes to control access to areas within the facility officially designated as publicly accessible;

**d.** Escort visitors and monitor visitor activity as identified in the escort policies for all visitors and visitor activities;

**e.** Retain visitor access records as required by IRD record retention policy and review visitor access records at least monthly;

**f.** Secure keys, combinations, and other physical access devices under their control; and

**g.** Inventory physical access devices and change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated or at least annually.

### 545.3.12.4 Access Control for Output Devices (PE-5)

Effective Date: 10/10/2017

The Agency must control physical access to information system output devices to prevent unauthorized individuals from obtaining the output. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas allowing access only to authorized individuals, and placing output devices in locations that can be monitored by organizational personnel.

### 545.3.12.5 Monitoring Physical Access (PE-6)

Effective Date: 10/10/2017

The Agency must:

**a.** Monitor physical access to facilities where information systems reside to detect and respond to physical security incidents;

**b.** Review physical access logs continuously and upon occurrence of alarms for attempted unauthorized access, rejected access attempts, and access outside of the working hours;

**c.** Coordinate results of reviews and investigations with the organizational incident response capability; and

**d.** Monitor physical surveillance equipment.

### 545.3.12.6 Access Control for Transmission Medium (PE-4) and Power Equipment and Cabling (PE-9)

Effective Date: 10/10/2017

The Agency must:

**a.** Ensure the protection of information system power equipment and power cabling from damage and destruction; and

**b.** Control physical access to transmission media, to include but not limited to locked wiring closets, disconnected or locked spare jacks, Protective Distribution Systems (PDS), and cabling by conduit or cable trays.

### 545.3.12.7 Emergency Shutoff, Power and Lighting (PE-10, 11, 12)

Effective Date: 10/10/2017

SOs must:

**a.** Coordinate with Agency designees or contractors to ensure an emergency shutoff capability for the information system or components;

**b.** Ensure emergency shutoff mechanisms are placed in a location that is protected but easily accessible;

**c.** Coordinate with Agency designees or contractors to ensure short-term uninterruptible power supply exists for the information system to facilitate an orderly shutdown of the information system in the event of a primary power source loss; and

**d.** Coordinate with Agency designees or contractors to ensure the existence and maintenance of emergency lighting where the information system is located. The emergency lighting must activate in the event of a power outage or disruption and must cover emergency exits and evacuation routes within the facility.

### 545.3.12.8 Fire Protection (PE-13)

Effective Date: 10/10/2017

SOs must coordinate with Agency designees or contractors to ensure that automated fire suppression and detection systems, supported by an independent energy source, are employed and maintained where the information system is located.

### 545.3.12.9 Temperature and Humidity Controls (PE-14)

Effective Date: 10/10/2017

SOs must coordinate with Agency designees or contractors to ensure that temperature and humidity levels within the facility where the information system is located are maintained and monitored continuously at levels consistent with manufacturer's requirements.

### 545.3.12.10 Water Damage Protection (PE-15)

Effective Date: 10/10/2017

SOs must coordinate with Agency designees or contractors to ensure that the information system is protected from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

### 545.3.12.11 Delivery and Removal (PE-16)
Effective Date: 10/10/2017

SOs must coordinate with Agency designees or contractors to ensure that information system components entering and exiting the facility are authorized and controlled and records of those items are maintained.

### 545.3.12.12 Alternate Work Site (PE-17)
Effective Date: 10/10/2017

The Agency must:

**a.** Coordinate with the CISO to identify, employ, and assess security controls at alternate work sites that are sufficient to protect information and information assets; and

**b.** Provide a means for employees to communicate with information security personnel or with M/CIO Service Now in case of security incidents or other problems.

## 545.3.13 Planning (PL)

### 545.3.13.1 Security Planning and Procedures (PL-1)
Effective Date: 10/10/2017

The CISO must ensure the development, implementation, dissemination, and annual review/update of a security planning policy and the procedures to implement it in compliance with applicable NIST standards.

SOs, in coordination with ISSOs and others as applicable, must document and implement security planning and procedures in accordance with this policy, including security-related activities affecting the information system.

### 545.3.13.2 System Security Plan (PL-2)
Effective Date: 10/10/2017

SOs must:

**a.** Develop security plans for the information system that:

**1)** Are consistent with the organization’s enterprise architecture;

**2)** Explicitly defines the authorization boundary for the system;

**3)** Describe the operational context of the information system in terms of Missions and business processes;

**4)** Provide the security categorization of the information system including supporting rationale;

**5)** Describe the operational environment for the information system and relationships with or connections to other information systems;

**6)** Provide an overview of the security requirements for the system;

**7)** Identify any relevant overlays, if applicable;

**8)** Describe the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions;

**9)** Are reviewed and certified by the CISO; and

**10)** Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

**b.** Review the security plan at least annually.

**c.** Update the plan to address changes to the information system or environment of operation and when problems with the IS are identified.

**d.** Protect the security plan from unauthorized disclosure and modification.

**e.** Distribute copies of the security plan and communicate subsequent changes to the plan at a minimum to the AO, DAOR, CISO and ISSO.

**f.** Plan and coordinate security-related activities affecting the information system with M/CIO/IA before conducting such activities in order to reduce the impact on other organizational entities.

### 545.3.13.3 Rules of Behavior (PL-4)

Effective Date: 10/10/2017

The CISO must develop, review annually, and update as required, the ROB for users requiring access to Agency information systems. The rules must:

**a.** Describe responsibilities and expected behavior with regard to information and information system usage;

**b.** Explicitly address restrictions associated with social media, posting Agency information to public web, and use of mobile devices; and

**c.** Explicitly address handling of PII and sensitive information.

SOs must establish, disseminate, and require signatures for a system-specific ROB, if required, but may utilize a generic ROB as long as the ROB addresses any issues specific to that system.

The CISO and SOs must:

**1)** Ensure that the ROBs are signed by users, indicating that they have read, understood, and agreed to abide by the ROB, before being granted access to information and information systems;

**2)** Require individuals who have signed a previous version of the ROB to read and re-sign when the ROB are revised/updated; and

**3)** Retain and make available the signed ROB for a minimum of two years.

For more information, see the **ROB for Users**.

### 545.3.13.4 Information Security Architecture (PL-8)

Effective Date: 10/10/2017

The CISO must:

**a.** Issue guidance and security requirements for all USAID systems;

**b.** Ensure that all systems comply with the USAID Enterprise Architecture (EA) and Security Architecture (SA); or

**c.** Provide mitigation controls for selected deficiencies to include a documented risk decision by the AO.

SOs must develop an information security architecture for the information system that:

**1)** Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

**2)** Describes how the information security architecture is integrated into and supports the enterprise architecture; and

**3)** Describes any information security assumptions and dependencies related to external services.

SOs must:

**a.** Review and update the information security architecture annually to reflect updates in the enterprise architecture; and

**b.** Ensure that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

### 545.3.14 Personnel Security (PS)

#### 545.3.14.1 Personnel Security Policy and Procedures (PS-1)
Effective Date: 10/10/2017

The Agency must create, document, disseminate, promulgate, review annually and update as required, a personnel security policy that addresses Position Risk Designation (PS-2), Personnel Screening (PS-3), Personnel Termination (PS-4), Personnel Transfer (PS-5), and Personnel Sanctions (PS-8).

The Agency must document, implement, and enforce procedures to comply with personnel security policy and associated personnel security controls. Such procedures must be reviewed annually and updated, as required.

Position risk designations must reflect Office of Personnel Management (OPM) policy and guidance (see **5 CFR 731.106** for details). For information regarding USAID personnel security policy, see **ADS 565, Physical Security Programs (Domestic)** and **ADS 566, Personnel Security Investigations and Clearances**.

#### 545.3.14.2 Access Agreements (PS-6)
Effective Date: 10/10/2017

The CISO or SOs must:

**a.** Develop and document access agreements for information systems.

**b.** Review and update the access agreements at least every three years.

**c.** Ensure that individuals requiring access to organizational information and information systems:

**1)** Sign appropriate access agreements prior to being granted access; and

**2)** Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or every three years.

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, and Rules of Behavior (ROBs), as well as conflict-of-interest agreements.

#### 545.3.14.3 Third Party Personnel Security (PS-7)

Effective Date: 10/10/2017

Third-party providers include, for example, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. ISSOs must ensure that SOs, CORs, or other designees:

**a.** Establish personnel security requirements including security roles and responsibilities for third-party providers;

**b.** Require third-party providers to comply with personnel security policies and procedures established by the Agency;

**c.** Document personnel security requirements;

**d.** Require third-party providers to notify the COR of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within one business day; and

**e.** Monitor provider compliance.

Accordingly, contracts with third party providers must include the appropriate clauses and contract requirements referenced in **ADS 302mah, Acquisition Guide for Unclassified Information System Security Systems and Services**.

### 545.3.15 Risk Assessment (RA)

#### 545.3.15.1 Risk Assessment Policy and Procedure (RA-1)

Effective Date: 10/10/2017

The CISO must develop, disseminate, review annually, and update as needed a risk assessment policy, as well as procedures for the policy's implementation.

#### 545.3.15.2 Security Categorization (RA-2)

Effective Date: 10/10/2017

**FIPS 199** establishes security categories for information systems based on the potential impact to the organization if certain events occur that affect the information systems. FIPS 199 defines potential impact levels as follows:

**a. Low:** The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

**b. Moderate:** The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

**c. High:** The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

SOs must:

**1)** Categorize information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The categorization decision must be approved by the CISO.

**2)** Document the security categorization results (including supporting rationale) in the security plan for the information system.

**3)** Ensure that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

### 545.3.15.3 Risk Assessment (RA-3)

Effective Date: 10/10/2017

The CISO must:

**a.** Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits, to include e-authentication risk assessments. Risk assessments must be conducted for all new technologies prior to use by the Agency;

**b.** Document risk assessment results in a risk assessment report;

**c.** Review risk assessment results at least annually and disseminate to system stakeholders; and

**d.** Update the risk assessment at least annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

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

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

SOs must implement the mitigations as established in the risk assessment in the timeframe identified by the associated risk level and/or submit risk acceptance

documentation to the AO.

### 545.3.15.4 Vulnerability Scanning (RA-5)

Effective Date: 10/10/2017

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.

M/CIO must do the following:

**a.** Deploy an Agency-wide network vulnerability scanning program. For more information, see the **USAID Continuous Monitoring Guide for Non-Cloud Systems** and the **USAID FedRAMP Continuous Monitoring Guide** (for Cloud Systems) (to obtain a copy of these documents, please go to **https://pages.usaid.gov/M/CIO/security-assessment-and-authorization-saa**).

**b.** Scan for vulnerabilities in the information system and hosted applications in accordance with the **USAID Continuous Monitoring Guide for Non-Cloud Systems** and the **USAID FedRAMP Continuous Monitoring Guide** (for Cloud Systems) at least monthly, and when new vulnerabilities potentially affecting the system/applications are identified and reported.

**c.** Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

**1)** Enumerating platforms, software flaws, and improper configurations;

**2)** Formatting checklists and test procedures; and

**3)** Measuring vulnerability impact.

**d.** Share information obtained from the vulnerability scanning process and security control assessments with CISO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

**e.** Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

**f.** Update the information system vulnerabilities scanned prior to a new scan or when new vulnerabilities are identified and reported.

**g.** Ensure that the information system implements privileged access authorization to all systems for all vulnerability scans.

SOs must:

**a.** Analyze vulnerability scan reports and results from security control assessments; and

**b.** Remediate legitimate vulnerabilities in accordance and in the timeframe identified by the associated risk impact level.

### 545.3.16 System and Services Acquisition (SA)

#### 545.3.16.1 System and Services Acquisition Policy and Procedures (SA-1)
Effective Date: 10/10/2017

The Agency must develop, document, and disseminate acquisition policies and procedures that address IT services and system acquisitions, and must review the policies and procedures at least annually and update, as applicable.

#### 545.3.16.2 Contractors and Outsourced Operations
Effective Date: 10/10/2017

The COR must coordinate with the CO and M/CIO to ensure that contracts involving IT include 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.

For all contracts involving IT, the contract requirements must address at a minimum:

**1)** How sensitive information and PII is to be handled and protected at contractor sites. This includes any information stored, processed, or transmitted using contractor information systems;

**2)** Personnel screening requirements;

**3)** Requirements for Agency authorization to operate and continuous monitoring; and

**4)** Incident response.

The COR must identify the IT requirements within the SOW and coordinate with the CO and M/CIO to ensure that the contract includes the appropriate clauses and contract requirements referenced in **ADS 302mah, Acquisition Guide for Unclassified Information System Security Systems and Services**.

This ensures 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.

### 545.3.16.3 Allocation of Resources (SA-2)

Effective Date: 10/10/2017

Information security is a very important business driver in this age of multiple threats to information systems throughout the government and private sphere. Any 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 **USAID Acquisition Regulation (AIDAR)** and **ADS 300, Agency Acquisition and Assistance (A&A) Planning** provide additional information on these requirements.

SOs must include information security requirements in their Capital Planning and Investment Control (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** and **ADS 577, Information Technology Capital Planning and Investment Control**.

### 545.3.16.4 System Development Life Cycle (SA-3)

Effective Date: 10/10/2017

The Agency must develop and establish an SDLC process that integrates the organizational information security risk management process into SDLC activities. SOs must manage information systems using the M/CIO SDLC standards that incorporate information security considerations, and must identify staff to perform security roles and responsibilities consistent with those identified in **545.2**.

### 545.3.16.5 Acquisition Process (SA-4)

Effective Date: 10/10/2017

SOs must ensure that the statement of work:

**a.** Includes the following for information systems and services:

**1)** Security requirements and controls for functional, strength, assurance, protection, and documentation, as well as user acceptance criteria; and

**2)** Requirements for development and operating environments.

**b.** Requires developers of IT systems, components, or services to :

**1)** Provide a description of the functional properties of the security controls to be employed and the functions, ports, protocols, and services required. Functional properties of security controls describe the functionality (i.e., security capability,

functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls;

**2)** Provide design and implementation information for the CISO and SO approved baseline security controls to be employed, at a minimum a high level design that documents all security-relevant external system interfaces;

**3)** Identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use;

**4)** Adhere to **ADS 302mak, USAID Implementation of Section 508 of the Rehabilitation Act of 1973**;

**5)** Employ only IT products on the **FIPS 201**-approved products list for Personal Identity Verification (PIV) or PIV-A capability implemented within organizational information systems. Exceptions must be approved by M/CIO with input from the CISO; and

**6)** When directed by the CISO or required by statute, ensure that IA or IA-enabled IT hardware, firmware, and software components or products incorporated into the Agency's information systems comply with the evaluation and validation requirements of the National IA Partnership (NIAP) Assurance Maintenance Program and/or **FIPS 140-2**.

For information on the cloud computing acquisition process, see **545.3.21.2, Cloud Computing**.

### 545.3.16.6 Information System Documentation (SA-5)

Effective Date: 10/10/2017

SOs must:

**a.** Include in the statement of work and/or service level agreements (SLA) a requirement to provide:

**1)** System administrator documentation that describes: secure configuration, installation, and operation of the system, component, and/or service; effective use and maintenance of security functions/mechanisms; and known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

**2)** User documentation that describes and provides instructions for user-accessible security functions/mechanisms.

**b.** Document attempts to obtain the documentation when such documentation is either unavailable or nonexistent, and must hold the contractor accountable as defined in

the contract; or must create the documentation internally.

**c.** Mark and protect documentation in accordance with the sensitivity level of the system or documentation and distribute the documentation to approved personnel.

### 545.3.16.7 Security Engineering Principles (SA-8)
Effective Date: 10/10/2017

M/CIO must define and document information system security engineering principles. SOs must conform to these information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

### 545.3.16.8 External Information System Services (SA-9)
Effective Date: 10/10/2017

SOs must:

**a.** Include in the statement of work, the requirement that providers of external information system services comply with organizational information security requirements and employ the SO and CISO approved baseline security controls;

**b.** Define and document government oversight and user roles and responsibilities with regard to external information system services;

**c.** Employ either NIST or USAID-defined continuous monitoring activities as agreed to in a continuous monitoring plan to monitor security control compliance by external service providers on an ongoing basis; and

**d.** Include in the statement of work, the requirement for providers of applicable external information systems to identify the functions, ports, protocols, and other services required for the use of such services.

### 545.3.16.9 Developer Configuration Management (SA-10)
Effective Date: 10/10/2017

SOs must:

**a.** Approve all changes to the information system.

**b.** Include in the statement of work, the requirement for developers of the information system to provide and follow an approved configuration management plan at a minimum, during development and operation. Configuration management plans must:

**1)** Address the integrity of changes for SO approved configuration items;

**2)** Implement only SO-approved changes, and document both the changes and the potential security impacts of such changes; and

**3)** Require that developers track security flaws and flaw resolution and report findings to the SO and ISSO.

### 545.3.16.10 Developer Security Testing and Evaluation (SA-11)

Effective Date: 10/10/2017

SOs must:

**a.** Include in the statement of work, the requirement for the developer of the information system, system component, or information system service to create and implement a security assessment plan;

**b.** Perform at a minimum system and regression testing/evaluation that includes, at a minimum, black box testing, and other testing at a level that is requested and approved by the CISO and consistent with the SO business needs;

**c.** Include in the statement of work, a requirement for the developer to produce supporting evidence and the results of the security testing/evaluation;

**d.** Implement a verifiable flaw remediation process; and

**e.** Correct flaws identified during security testing/evaluation.

## 545.3.17 System and Communications Protection (SC)

### 545.3.17.1 System and Communications Protection Policy and Procedures (SC-1)

Effective Date: 10/10/2017

The CISO must:

**a.** Develop, document, and disseminate a system and communications protection policy to USAID staff that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

**b.** Review the policy at least annually and update as required;

**c.** Develop procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

**d.** Review procedures at least annually and update as required.

### 545.3.17.2 Application Partitioning (SC-2)

Effective Date: 10/10/2017

SOs must ensure that the information system separates user functionality (including user interface services) from information system management functionality. Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.

### 545.3.17.3 Information in Shared Resources (SC-4)

Effective Date: 10/10/2017

SOs must configure the information system to prevent unauthorized and unintended information transfer via shared system resources.

### 545.3.17.4 Denial of Service Protection (SC-5)

Effective Date: 10/10/2017

SOs must ensure that information systems, to include wireless devices and endpoints, protect against or limits the effects of internal and external denial of service attacks by employing M/CIO and CISO approved safeguards.

### 545.3.17.5 Boundary Protection (SC-7)

Effective Date: 10/10/2017

SOs must configure the information system to:

**a.** Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system;

**b.** Implement sub-networks for publicly accessible system components that are physically and logically separated from internal organizational networks;

**c.** Connect to external networks or information systems only through managed interfaces consisting of CISO-approved boundary protection devices and must limit the number of external network connections to the information system;

**d.** Implement managed interfaces for each external telecommunication service;

**e.** Establish a traffic flow policy for each managed interface;

**f.** Protect the confidentiality and integrity of the information being transmitted across each interface;

**g.** Document each exception to the traffic flow policy with a supporting Mission/business need and duration of that need;

**h.** Review exceptions to the traffic flow policy at least annually and remove exceptions

that are no longer supported by an explicit Mission/business need;

**i.** Configure managed interfaces to deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

**j.** In conjunction with a remote device, prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks; and

**k.** Implement host-based boundary protection for mobile endpoints.

#### 545.3.17.6 Transmission Confidentiality and Integrity (SC-8)
Effective Date: 10/10/2017

SOs must ensure that the information system protects the confidentiality and integrity of transmitted information. The information owner (IO) may require additional controls for protection of information integrity.

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and detect changes to information during transmission unless otherwise protected by mechanisms approved by CISO in writing.

#### 545.3.17.7 Network Disconnect (SC-10)
Effective Date: 10/10/2017

SOs must ensure the information system terminates the network connection associated with a communications session at the end of the session or after 60 minutes of inactivity (see **545.3.2.9**, Session Lock and Termination (AC-11 and AC-12), for logical session terminations).

#### 545.3.17.8 Cryptographic Key Establishment and Management (SC-12)
Effective Date: 10/10/2017

When cryptography is required, SOs must establish and manage all cryptographic keys employed within the information system in accordance with CISO-defined requirements for key generation, distribution, storage, access, and destruction, and when explicitly approved by M/CIO.

#### 545.3.17.9 Cryptographic Protection (SC-13)
Effective Date: 10/10/2017

SOs must ensure that the information system implements only M/CIO and CISO approved cryptographic technologies that conform to FIPS-validated standards.

#### 545.3.17.10 Collaborative Computing Devices (SC-15)
Effective Date: 10/10/2017

SOs must prohibit all remote activation and/or use of collaborative computing devices, such as video/audio conferencing, networked white boards, cameras, and microphones, unless explicitly authorized in writing by the M/CIO and CISO.

If remote activation or use is authorized, SOs must ensure the information system provides an explicit indication of use and requests permission from the user who is physically present at the collaborative computing device.

The use and installation of collaboration software is strictly prohibited unless approved by M/CIO. When collaboration software is authorized by M/CIO, the remote control capability must be disabled. When processing information using collaborative software, information owners must establish and maintain access permissions/rights to ensure that only authorized users can access the information.

#### 545.3.17.11 Public Key Infrastructure Certificates (SC-17)

Effective Date: 10/10/2017

SOs must only issue public key certificates or use public key service providers that are authorized and approved by the M/CIO and CISO.

#### 545.3.17.12 Mobile Code (SC-18)

Effective Date: 10/10/2017

CISO and SOs must define acceptable and unacceptable usage policies for mobile code and mobile code technologies, such as JavaScript, VBScript, Java applets, ActiveX controls, and Flash animations. These policies must:

**a.** Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies;

**b.** Authorize, monitor, and control the use of mobile code within the information system; and

**c.** Identify unacceptable mobile code and take the necessary corrective action when such code is detected.

#### 545.3.17.13 Voice Over Internet Protocol (SC-19)

Effective Date: 10/10/2017

SOs, in coordination with the CISO, must:

**a.** Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

**b.** Authorize, monitor, and control the use of VoIP within the information system.

### 545.3.17.14 Secure Name/Address Resolution Service (Authoritative Source) (SC-20)

Effective Date: 10/10/2017

SOs must configure the information system to:

**a.** Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries. Additional artifacts include, for example, Domain Name Service (DNS) Security (DNSSEC) digital signatures and cryptographic keys.

**b.** Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in DNS.

SOs who employ technologies other than DNS to map between host/service names and network addresses must provide a detailed implementation description in the system's security plan. For more information, see **OMB Memorandum 08-23**.

### 545.3.17.15 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21)

Effective Date: 10/10/2017

SOs must ensure that the information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SOs who employ technologies other than DNS must obtain approval from M/CIO and CISO and must provide a detailed implementation description in the system's security plan.

### 545.3.17.16 Architecture and Provisioning for Name/Address Resolution Service (SC-22)

Effective Date: 10/10/2017

SOs must ensure that information systems that provide name/address resolution service are fault-tolerant and implement internal/external role separation.

### 545.3.17.17 Session Authenticity (SC-23)

Effective Date: 10/10/2017

SOs must ensure that Information systems protect the authenticity of communications sessions by using approved TLS or SSL certificates to prevent threats such as man-in-

the-middle attacks, session hijacking, and insertion of false information.

### 545.3.17.18 Protection of Information at Rest (SC-28)
Effective Date: 10/10/2017

SOs must protect the confidentiality and integrity of sensitive data at rest, to include at a minimum PII, on mobile devices, endpoints, and databases identified as high value IT assets.

- Mobile devices and endpoints must be protected with **FIPS 140-2** compliant encryption; and

- Databases must be protected at least with transparent data (TD) type encryption.

### 545.3.17.19 Process Isolation (SC-39)
Effective Date: 10/10/2017

SOs must ensure that the information system maintains a separate execution domain for each executing process. This capability is available in most commercial operating systems that employ multi-state processor technologies.

### 545.3.18 System and Information Integrity (SI)
Effective Date: 10/10/2017

System and Information Integrity is the assurance that business data has not been tampered with, altered, or damaged. System and Integrity controls apply to all USAID endpoints to the extent that is practical to include workstations, laptops, servers, and netbooks.

### 545.3.18.1 System and Information Integrity Policy and Procedures (SI-1)
Effective Date: 10/10/2017

The CISO must develop, disseminate to USAID staff with a need to know, review annually, and update as applicable a system and information integrity policy.
SOs must document, review annually, and update as applicable procedures, and implement and enforce those procedures to comply with system and integrity policy and associated controls.

### 545.3.18.2 Flaw Remediation (SI-2)
Effective Date: 10/10/2017

M/CIO must employ automated mechanisms that scan monthly to determine the state of information system components with regard to flaw remediation.

SOs must:

**a.** Identify, report, and correct information system flaws;

**b.** Test software updates related to flaw remediation for effectiveness and potential side effects on Agency information systems before installation;

**c.** Incorporate flaw remediation into the configuration management process; and

**d.** Install security-relevant software and firmware updates within timelines defined in the M/CIO vulnerability management procedures.

### 545.3.18.3 Malicious Code Protection (SI-3)
Effective Date: 10/10/2017

M/CIO must employ, centrally manage, and update (to include signature files) malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

The protection mechanisms must perform the following scans:

**a.** Continuous scans of the information system;

**b.** Real-time scans of files from external sources at endpoints and network entry/exit points as the files are downloaded, opened, or executed; and

**c.** Scans must block or quarantine malicious code in response to malicious code detection.

SOs must address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

### 545.3.18.4 Information System Monitoring (SI-4)
Effective Date: 10/10/2017

The CISO and SOs must monitor events on information systems to detect and identify indicators of potential attacks and unauthorized use, and unauthorized local, network, and remote connections. This must be done in accordance with the **USAID Information Security Continuous Monitoring Strategy** and the **IA Audit and Accountability Guide** (to obtain copies of these documents, please go to **https://pages.usaid.gov/M/CIO/security-assessment-and-authorization-saa** or send an email to **ato@usaid.gov**).

SOs must:

**a.** Deploy monitoring devices strategically within the information system to collect organization-determined essential information;

**b.** Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

**c.** Heighten the level of information system monitoring activity whenever the CISO indicates there is an increased risk to organizational operations and assets, individuals, or other organizations, based on law enforcement information, intelligence information, or other credible sources of information;

**d.** Obtain legal opinion, in coordination with CISO, with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. All information is protected under the Privacy Act of 1974 and in accordance with **ADS 508, The USAID Privacy Policy**;

**e.** Provide audit logs to ISSOs and CISO, as needed;

**f.** Ensure the information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions;

**g.** Ensure the information system alerts ISSOs when the following indications of compromise or potential compromise occur, as defined in the **USAID Information Security Continuous Monitoring Strategy** and the **IA Audit and Accountability Guide** (to obtain copies of these documents, please go to **https://pages.usaid.gov/M/CIO/security-assessment-and-authorization-saa** or send an email to **ato@usaid.gov**); and

**h.** Coordinate with the CISO to ensure the information system has a capability to discover, collect, distribute, and use indicators of compromise.

M/CIO must:

**1)** Deploy monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization;

**2)** Employ automated tools to support near real-time analysis of events;

**3)** Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system; and

**4)** Make provisions so that selected encrypted communications traffic to external destinations is visible to CISO-authorized monitoring tools.

### 545.3.18.5 Security Alerts, Advisories, and Directives (SI-5)

Effective Date: 10/10/2017

The CISO must:

**a.** Obtain information system security alerts, advisories, and directives from US-CERT, OMB, and other designated organizations with the responsibility and authority to

issue such directives on an ongoing basis;

**b.** Generate internal security alerts, advisories, and directives as deemed necessary;

**c.** Disseminate security alerts, advisories, and directives to USAID staff and US-CERT, as well as other designated organizations with the responsibility and authority to receive such alerts, advisories, and directives; and

**d.** Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

### 545.3.18.6 Software, Firmware and Information Integrity (SI-7)

Effective Date: 10/10/2017

M/CIO must employ integrity verification tools to detect unauthorized changes or modifications to software or firmware in the USAID network.

SOs must ensure that the information system:

**a.** Performs an integrity check minimally at startup and at the request of the CISO upon the identification of a new and relevant threat; and

**b.** Reports the detection of unauthorized changes to security logs and elevated privilege changes in accordance with the CISO incident response plan.

### 545.3.18.7 Spam Protection (SI-8)

Effective Date: 10/10/2017

M/CIO must employ and centrally manage an enterprise spam protection mechanism.

SOs must:

**a.** Employ or ensure spam protection mechanisms at information system entry and exit points and at workstations, servers, and 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. Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers; and

**b.** Update or ensure automatic updates to spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

### 545.3.18.8 Information Input Validation (SI-10)

Effective Date: 10/10/2017

SOs must ensure that the information system checks the validity of SO-defined input values. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

### 545.3.18.9 Error Handling (SI-11)
Effective Date: 10/10/2017

SOs must ensure that the information system:

**a.** Generates 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

**b.** Reveals error messages only to explicitly authorized staff.

### 545.3.18.10 Information Handling and Retention (SI-12)
Effective Date: 10/10/2017

SOs must handle and retain information within the information system as well as output from the system in accordance with **ADS 502, The USAID Records Management Program** and **545.3.11**, Media Handling.

### 545.3.18.11 Memory Protection (SI-16)
Effective Date: 10/10/2017

SOs must ensure that the information system implements hardware or software enforced data execution prevention safeguards to protect its memory from unauthorized code execution.

## 545.3.19 Other USAID-Specific Policies

### 545.3.19.1 Acceptable Use
Effective Date: 10/10/2017

M/CIO established an acceptable use policy as well as disciplinary actions for misuse of IT resources, to include email, Internet, and Intranet, and must take steps to ensure that the USAID workforce use these services in accordance with policy.

**a.** Members of the workforce must adhere to the security policy contained in this chapter, and the plans, procedures, ROB, agreements, standards, checklists, and guidelines derived from policy (see **Acceptable Use Policy for IT Resources**, **ADS 549, Telecommunications Management**, **ADS 541, Information Management**, and **ROB for Users**).

**b.** The workforce must adhere to CIO ROB and CISO policy on the acceptable use of BYOD and applications that properly isolate and contain USAID information. Personal online content storage such as iCloud, Dropbox, and OneDrive are

prohibited for storing USAID information.

**c.** Members of the workforce must not use personal electronic messaging accounts, including personal email, text, or chat, to conduct official USAID business. Only official government electronic messaging is permitted. The following policy statements apply to the use of electronic messaging accounts:

- Non-official electronic messaging (such as personal Gmail, Yahoo, and AOL, and email accounts ending in .com, .net, .org, etc.) must not be used to transmit, process, or store Agency-owned or other official government information. For email, official government electronic messaging accounts end with a .gov or .mil extension. Email accounts that end in anything other than .gov or .mil may not be used unless there is an exceptional circumstance. An exceptional circumstance is defined as an emergency situation, such as a catastrophic natural disaster, severe or extreme weather conditions such as a flood or tornado, a national security event, or a regional power loss of six hours or more.

- In the rare circumstance in which the security of standard communication channels is at risk and use of non-official electronic messaging is deemed to be the only option, a waiver must be requested, as follows:

  **1)** A staff member, Bureau, Independent Office, or Mission must contact the M/CIO Service Desk at **cio-helpdesk@usaid.gov** to formally request consideration for an exception from M/CIO.

  **2)** The M/CIO Service Desk provides the format for an Information Memo to the CIO that the requestor must complete and identifies to whom it should be submitted in M/CIO (e.g., M/CIO Chief of Staff).

  **3)** M/CIO reviews the Exception Request and issues a final decision on whether it meets the criteria to apply the exception rule.

  **Note:** Government email must be used unless a waiver is granted by M/CIO. This policy is enforceable under federal law and violators may be prosecuted.

  - Staff must follow the standards and procedures outlined in Acceptable Use Policy for IT Resources.

  - Auto-Forwarding or redirecting email or other electronic communications to addresses outside of the .gov or .mil domain is prohibited. Users may forward low-risk messages manually.

  - When sending electronic messages outside of the .gov or .mil domain, staff must ensure that any sensitive information, particularly PII data elements, is attached as an encrypted file using M/CIO-

approved encryption technologies. Such transmissions should only be made in the performance of official duties.

See **ADS 502, The USAID Records Management Program** for guidance on electronic messaging and exceptional circumstances.

**d.** Staff must not participate in unethical, illegal, or inappropriate activities for conducting official business or while using government resources. These activities include, but are not limited to, pirating software, stealing passwords and credit card information, and viewing/exchanging inappropriate written or graphic material (i.e., pornography).

**e.** Staff must protect Personally Identifiable Information (PII) and sensitive information to the greatest extent feasible in accordance with this policy and federal laws.

**f.** Staff should have no expectation of privacy when using government resources. All GFE equipment and equipment operated on behalf of USAID, is subject to monitoring in accordance with this policy (Section **545.3.18.4**, Information System Monitoring (SI-4)); however, all PII is protected under the **Privacy Act of 1974** and in accordance with **ADS 508, The USAID Privacy Policy**.

**g.** **Intellectual Property Management**: Intellectual property is defined as intangible property, such as patents, trademarks, and copyrighted materials which are the result of intellectual effort and are under legal protection. Management must ensure the proper handling of such information.

All information processed, generated, or stored on any USAID information system is the property of USAID. Staff requiring access to a USAID information system or USAID sensitive or proprietary information must sign a Non-Disclosure Agreement (NDA). 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.

### 545.3.19.2 Information Security Policy Violation and Disciplinary Action

Effective Date: 10/10/2017

Staff who commit policy infractions, intentional or unintentional, including misuse of USAID IT resources, may be subject to disciplinary actions as defined in **ADS 485, Disciplinary Action - Foreign Service** or **ADS 487, Disciplinary and Adverse Actions Based Upon Misconduct - Civil Service**.

These sanctions may include counseling, remedial training, revocation of access privileges, and possibly termination. Contractor employees can have their access privileges revoked and the contract itself could be terminated as a result of an infraction. When such actions appear to be criminal in nature, the matter must be referred to the USAID Office of the Inspector General (OIG).

### 545.3.20 Prohibited and Restricted Use of Technologies
Effective Date: 10/10/2017

USAID prohibits or restricts certain activities and the use of certain technologies that introduce threats or exceptionally high risks to the Agency. The following technologies or activities are prohibited or restricted unless explicitly authorized by M/CIO:

- Audio or video streaming;
- Peer-to-peer software or music sharing/piracy;
- Visiting online gaming, gambling, and pornography sites;
- Viewing of offensive content;
- Hacking;
- Use of freeware, shareware, file-sharing and open source software must be approved by the CISO. Approval is based on an assessment of risk and the total life cycle cost (see **OMB Memo M-04-16, Software Acquisition** for acquisition guidance for this type of software); and
- Use of instant messaging software.

#### 545.3.20.1 Social Media and Social Networking
Effective Date: 10/10/2017

Social media sites can be internally hosted/developed solutions or hosted by external commercial services, contracted for use by the Agency. Examples of social media include Internet forums, videos, wikis, blogs, virtual worlds, podcasts, and social networking sites. The following policy statements apply to social media and networking applications intended for Agency use (see **ADS 558, Use of Social Media For Public Engagement**):

**a.** Social media and networking applications must not be used without written approval from M/CIO. This approval may be in the form of an authority to operate (ATO), risk decision memorandum based on a risk assessment, and/or M/CIO SAR approval. **Note:** Refer to **545.3.13.3**, Rules of Behavior (PL-4), letter “b”, for the main guidance on this subject.

**b.** The CISO must develop training material on the use of approved social media and networking applications.

**c.** Staff must not post sensitive information, 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.

**d.** SOs, CORs, or others responsible for social media/networking applications must ensure via contracts or other agreements, that the records are retained consistent with the Agency records retention requirements (as defined in **ADS 502, The USAID Records Management Program**).

**e.** Only LPA-designated personnel may post content on behalf of the Agency or be granted access to the site on a continuing basis.

**f.** Posted content must follow Agency and vendor Terms of Service (ToS) guidelines. Contact LPA for the ToS and guidelines for posting to these sites.

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

**1)** Staff using social media technologies in an official capacity must do so only on Agency-approved accounts and may only use official email or other official contact information to create and manage such accounts.

**2)** When directed by M/CIO as a condition of use, SOs must obtain approval from the Office of General Council (GC) for a cloud service provider's ToS agreement. M/CIO must verify GC approval prior to authorizing use.

**3)** Staff must not post any official Agency positions on social media sites unless explicitly authorized by LPA. This does not include sharing or reposting of official Agency positions.

**4)** Staff must ensure that the content maintained on their social media sites is secure and adequately safeguarded from unauthorized modification or destruction.

**5)** Content must not be posted to any social media site for which the Agency has not approved and published final posting guidelines and ToS.

**6)** Content managers must review and understand the appropriate Agency-level ToS for the appropriate social media host.

**7)** Content managers must make a risk decision prior to posting any information. They must recognize that social media 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.

**8)** With social media comes the ability to comment and engage directly with the public. Postings in that case must be carefully vetted with LPA in USAID/W, with the Development Outreach Coordinator in Missions and with B/IO leadership before responding to comments.

### 545.3.20.2 Mobile Devices

Effective Date: 10/10/2017

Mobile Device (MD) security must adhere to standards defined in **NIST SP 800-124**. The following policy statements apply to MDs (see **545.3.2.13**, Access Control for Mobile Devices (AC-19); and **545.3.17.12**, Mobile Code (SC-18); and contact M/CIO/IA for further guidance):

**a.** If a user knows or suspects that an MD has been compromised, the user must immediately turn off the MD and notify the M/CIO Service Desk at **cio-helpdesk@usaid.gov**. The user must not allow the MD to connect to any networks (wireless or wired) or GFE.

**b.** SOs must provide extra precautions for all MD users to take in order to compensate for the lack of physical security controls when traveling with MDs.

**c.** M/CIO, in coordination with the CISO, must develop and implement a mobile security architecture that specifically addresses centralized management and security issues for mobile and wireless technologies, to include incidents, secure configurations, application management, anti-malware/virus, and denial of service.

**d.** Personnel with GFE MDs must sign applicable M/CIO access agreements acknowledging they have read, understood, and agreed to abide by the constraints associated with organizational information systems to which access is authorized.

**e.** SOs must only procure and allow use of GFE MDs that:

**1)** Allow secure configurations as defined by M/CIO,

**2)** Prohibit alterations, and

**3)** Can be centrally managed by M/CIO.

**f.** Staff must not physically connect non-GFE MDs to the USAID networks or information systems.

**g.** MDs must not be used to store, process, or transmit combinations, PINs, or sensitive information in unencrypted formats.

**h.** M/CIO must approve the use and maintain a current inventory of all approved wireless MDs in operation, and SOs must document system specific use in the SSP to include explicit approval or denial to process, store, or transmit sensitive information.

**i.** Wireless MDs must be sanitized by M/CIO, using CISO approved methods before reuse by another individual, office, or Bureau within USAID, or before they are made surplus, returned to the manufacturer, or disposed.

**j.** Legacy wireless MDs not compliant with USAID information security policy must be phased out and replaced via an M/CIO approved transition plan. This plan must describe the provisions, procedures, and restrictions for transitioning these wireless MDs to USAID approved devices. Continued operation of these noncompliant systems requires an approved exception from the CISO and AO.

#### 545.3.20.3 Wireless Network Communications and Systems
Effective Date: 10/10/2017

The following policy statement applies to wireless network communications:

**a.** Only CIO and CISO-approved Wireless network communication and application technologies, including any wireless tactical systems, are authorized for use within USAID; and

**b.** SOs must establish usage restrictions and implementation guidance for wireless technologies and authorize, monitor, and control wireless access to USAID information systems.

### 545.3.21 Other Technologies

#### 545.3.21.1 Third-Party Web Sites
Effective Date: 10/10/2017

Third-party Web sites are sites funded by the Agency, 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 (see **ADS 557, Public Information**). The following policies apply to these Web sites:

**a.** **Approval**. All third-party Web sites must be evaluated and approved by the LPA Web Site Governance Board (**webgovernanceboard@usaid.gov**) prior to site development.

**b.** **Third-Party Privacy Policies**. For guidance on Third-Party Privacy Policies please see **ADS 508.3.5.2** and **ADS 508.3.10.5**.

**c.** **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.

**d.** **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.

**e.** **Information Collection**. Regarding the use of third-party Web sites or applications, the COR is responsible for coordinating with the CO to ensure that contract terms

restrict contractors to collecting only the amount of information necessary to complete the specific business need as required by statute, regulation, or Executive Order (see **ADS 302, USAID Direct Contracting**).

### 545.3.21.2 Cloud Computing

Effective Date: 10/10/2017

Cloud computing is a model for enabling convenient and 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. The following policy statements apply to cloud-based solutions (contact M/CIO/IA for additional guidance):

**a.** All cloud-based systems/services must meet requirements defined by the Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework or other requirements as defined by M/CIO. For more information, see the **USAID FedRAMP Continuous Monitoring Guide**.

**b.** The SO and/or COR must coordinate with the CO and M/CIO to ensure that the appropriate security requirements are included in the contracts and/or SLAs for cloud-based services and systems. The clauses and special contract requirements referenced in **ADS 302mah, Acquisition Guide for Unclassified Information System Security Systems and Services** include requirements for:

- Regulatory Compliance (FISMA, Privacy Act),
- Personnel Security Requirements,
- Data ownership and portability,
- Location of Data,
- Data Segregation,
- Audit Logs,
- Data Retention,
- Records management and electronic discovery,
- Forensics,
- Incident Management Backups,
- Contingency Planning, including alternate site processing/storage agreements,

- Configuration Management,
- Vulnerability Management, and
- Agreement termination and data retrieval.

**c.** Cloud-based services must not be used without expressed written approval from M/CIO. This approval may be in the form of an ATO, risk decision memorandum based on a risk assessment, and/or M/CIO SAR approval.

**d.** The security controls outlined in this policy apply to all cloud-based services. This includes M/CIO approval processes, all phases of the risk management framework and privacy requirements.

**e.** All public cloud-based computing solutions must comply with **NIST SP 800-144**.

### 545.3.22 PII and Sensitive Information

Effective Date: 10/10/2017

Sensitive information, including PII, is collected, used, maintained and shared by USAID staff to enable the Agency's global mission. Staff must take steps to provide protection for sensitive information to include PII. This section provides an overview of what information is considered sensitive. Guidance on how to protect such information, and Agency resources for additional information, can be found in **ADS 508, The USAID Privacy Policy** and throughout this ADS chapter.

#### 545.3.22.1 Types of Sensitive Information

Effective Date: 10/10/2017

To protect sensitive information, staff must be aware of the various types of sensitive information as well as the levels of protection required for each. Sensitive information must be marked as Sensitive But Unclassified (SBU) with subcategory markings as needed. Sensitive information includes but is not limited to:

**a.** PII (see **ADS 508**), including information protected under the Privacy Act of 1974;

**b.** Personal Health Information (PHI) and any information protected under the Health Insurance Portability and Accountability Act of 1996;

**c.** Information protected by Nondisclosure Agreement (i.e., Agency proprietary information);

**d.** Human resource information, including personal files, educational, and financial records;

**e.** Staff travel information;

**f.** Business proprietary information given to USAID as part of contracts or agreements;

**g.** Procurement sensitive information;

**h.** Statutorily protected information (e.g., International Traffic in Arms [ITAR]);

**i.** Law enforcement sensitive;

**j.** Security information, to include clearance and badging information; and

**k.** Other information identified by the information owner and Agency policy or programs as sensitive.

Sensitive information must be marked and handled appropriately. In addition, national security and other classified information have greater sensitivities and must be handled according to regulations.

### 545.3.23 Waivers
Effective Date: 10/10/2017

A waiver is the written permission required to temporarily or permanently eliminate the requirements of a specific policy or control. Examples of exceptions include legacy or end of life systems, or systems where implementing certain security controls may impact critical Mission functions or may not be cost effective.

In all cases, SOs should seek to implement the minimum necessary controls as outlined by NIST and M/CIO defined compensating controls. For cases where information systems cannot fully comply with policy and regulatory requirements due to a business need, SOs may request a waiver in writing from the CISO.

## 545.4 MANDATORY REFERENCES

### 545.4.1 External Mandatory References
Effective Date: 10/10/2017

**a.** **5 Code of Federal Regulations (CFR) 731.106, Designation of Public Trust Positions and investigative Requirements, January 2012**

**b.** **Agency for International Development Acquisition Regulation (AIDAR)**

**c.** **Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service**

**d.** **EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011**

**e.** Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, October 2010

**f.** FIPS 197, Advanced Encryption Standard (AES), November 26, 2001

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

**h.** FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors

**i.** Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003

**j.** HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004 (Authority)

**k.** National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience

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

**m.** 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)

**n.** NIST SP 800-18 Rev 1, Guide for Developing Security Plans for Information Technology Systems, February 2006

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

**p.** NIST SP 800-37 (rev. 1), Guide to Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010

**q.** NIST SP 800-39, Managing Information Security Risk, March 2011

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

**s.** NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (supersedes NIST SP 800-26)

**t.** NIST SP 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, June 2010

u. NIST SP 800-55, Rev. 1, Performance Management Guide for Information Security, July 2008

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

w. NIST SP 800-63, Electronic Authentication Guideline, Revision 2, August 2013

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

y. NIST SP 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise, Revision 1, June 2013

z. NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011

aa. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing

ab. NIST 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials, December 2014

ac. NIST Description, The United States Government Configuration Baseline (USGCB), March 7, 2010

ad. NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization

ae. OMB Circular No. A-123

af. OMB Circular No. A-130 (July 2016)

ag. OMB Enterprise Architecture Assessment Framework

ah. OMB Memorandum 08-23, Securing the Federal Government's Domain Name System Infrastructure, August 23, 2008

ai. Pub. L. 113-283, Federal Information Security Modernization Act of 2014 (FISMA), December 8, 2014

aj. Pub. L. 107-347, Federal Information Security Modernization Act of 2002 (FISMA) (Title III of the E-Government Act of 2002), December 2002, as amended (Authority)

**ak.** U.S. Government Configuration Baseline (USGCB) CIO Council Memorandum, USGCB Highlights, September 15, 2010

### 545.4.2 Internal Mandatory References

Effective Date: 10/10/2017

**a.** ADS 103, Delegations of Authority

**b.** ADS 302mak, USAID Implementation of Section 508 of the Rehabilitation Act of 1973

**c.** ADS 485, Disciplinary Action - Foreign Service

**d.** ADS 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct - Civil Service

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

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

**g.** ADS 508, USAID Privacy Policy

**h.** ADS 519, Building Support Services in USAID/Washington

**i.** ADS 541, Information Management

**j.** ADS 542, Planning and Budgeting for Information Technology (IT) Resources

**k.** ADS 545mai, Business Continuity Planning Procedures and Guidelines

**l.** ADS 545mak, Data Remanence Procedures

**m.** ADS 545mal, Disaster Recovery Planning Procedures and Guidelines

**n.** ADS 545mam, Email Acceptable Usage Policy

**o.** ADS 545man, Establishing System Security Level Procedures and Guidelines

**p.** ADS 545map, Incident Identification and Reporting Procedures

**q.** ADS 545maq, Information Assurance Procedures

**r.** ADS 545mar, Internet Acceptable Usage Policy

**s.** ADS 545mau, Password Creation Standards

**t.** ADS 545max, Access Procedures and Guidelines for Information Technology

(IT) Telecommunications (Telecom) Closets

u. ADS 545may, Risk Assessment Guidelines

v. ADS 545mbd, Rules Of Behavior for Users

w. ADS 545mbf, Information System Security Virus Detection Guidelines

x. ADS 545mbm, Guidelines for Remote Access Soft Tokens for Personal Devices

y. ADS 547, Property Management of Information Technology (IT) Resources

z. ADS 549, Telecommunications Management

aa. ADS 552, Classified Information Systems Security

ab. ADS 557, Public Information

ac. ADS 558, Use of Social Media For Public Engagement

ad. ADS 559, Inquiries from the News Media

ae. ADS 560, News Releases and Services

af. ADS 562, Physical Security Programs (Overseas)

ag. ADS 565, Physical Security Programs (Domestic)

ah. ADS 566, Personnel Security Investigations and Clearances

ai. ADS 569, Counterintelligence Program

aj. ADS 577, Information Technology Capital Planning and Investment Control

ak. M/CIO Strategic Planning and Enterprise Architecture

al. **USAID FISMA Program document** (to obtain a copy of this document, please send an email to **ato@usaid.gov**)

am. **USAID Incident Response Program Concept of Operations (CONOPS)** (to obtain a copy of this document, please send a request to the M/CIO Service Desk at **cio-helpdesk@usaid.gov**)

an. USAID Plan of Action and Milestones (POA&M) Management Guide

**ao. USAID Vulnerability Management Standard Operating Procedure (SOP)** (to obtain a copy of this document, please send a request to the M/CIO Service Desk at **cio-helpdesk@usaid.gov**)

## 545.5 ADDITIONAL HELP

Effective Date: 10/10/2017

**a.** **ADS 545sah, Warning Screen Messages Guidelines**

**b.** **IDmanagement.gov**

## 545.6 DEFINITIONS

Effective Date: 10/10/2017

See the **ADS Glossary** for all ADS terms and definitions.

**802.11**
This 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, and released the most recent updates in 2012 and 2013. (**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. (**Chapter 545**)

**asset (IT)**
An IT-related item/resource that has value to an organization, including, but not limited to, another organization, person, computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform, and related hardware (e.g., locks, cabinets, keyboards). (NIST IR 7693 Asset Identification [IR 7693]) (**Chapter 545**)

**audit**
An independent review and examination of system controls, records and activities. (**Chapter 545**)

**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**)

**authority to operate (ATO)**
The formal declaration by the DAA that an Information System is approved to operate using a prescribed set of safeguards. (**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. (**Chapter 545** and **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 (i.e., 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**)

**Business Owner**

A Business Owner has varying responsibilities depending on the Mission or Business or Information Owner. In general, Business Owners are responsible for ensuring the mission of the organization is accomplished. In some cases, Business Owners are responsible for funding and other resources that support their line of business. (ISSO Handbook) (**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**)

**Commercial-off-the-Shelf (COTS)**
A Federal Acquisition Regulation (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**)

**common secure configurations**
These provide recognized, standardized benchmarks that stipulate secure configuration settings for specific information technology platforms/products and

instructions for configuring those information system components to meet operational requirements. Common secure configurations include the United States Government Configuration Baseline (USGCB), which affects the implementation of several AC and CM controls. (**Chapter 545**)

**compensating control**
A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time. (**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**)

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

**configuration settings**
The set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture or functionality of the system. All organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline. See also **security-related parameters** and **common secure configurations.** (**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 any U.S. citizens who are employed as Personal Service Contractors (PSC), independent contractors, fellows, institutional contractors, 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. (**Chapter 545** and **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 by the owner's copyright. (**Chapter 545**)

**critical infrastructure**
Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (**National Infrastructure Protection Plan 2013**) (**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 SEC. 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**)

**Demilitarized 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, and email servers. The term comes from military use, meaning a buffer area between two enemies. (**Chapter 545**)

**Denial of Authorization to Operate (DATO)**
Is determined when the Agency Authorizing Official (AO) (Chief Information Officer), after reviewing the authorization package, determines that the risk to organizational operations and assets, individuals, other organizations, and the nation is unacceptable and immediate steps cannot be taken to reduce the risk to an acceptable level. The Agency AO issues a DATO for the information system or for the common controls inherited by organizational information systems. When a DATO is issued, the information system is not authorized to operate, or if the

system is in operation, all activity is halted. (**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 the act of transforming information into an unintelligible form, specifically to obscure its meaning or content. (**Chapter 545**)

**endpoint and mobile devices**
Endpoint devices are servers, workstations (desktops), laptops, and net-books. Mobile devices are not considered to be endpoints. Mobile devices are Blackberry phones, iPhones, Android phones, and tablets. Both endpoint and mobile devices are hardware assets but they are separate and counted separately. (**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 527**, **535**, **545**)

**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 302**, **330**, **545**)

**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)**
*(Amended in 2014 [see below]* (44 USC § 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 Information Security Modernization Act of 2014 (FISMA)**
(44 USC § 3541, et seq.). Amends the Federal Information Security Management Act of 2002 (FISMA), the law that oversees the security of the Federal Government's information technology systems. The new bill will codify and clarify the existing roles and responsibilities of the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) for information security. It also updates guidelines that federal agencies should follow in the event that there is an unauthorized release of data. (**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-sharing software**
File-sharing software is also known as peer-to-peer file sharing software; such software allows the user to download files from a network of "peers". File-sharing software poses a major threat to USAID information because of its anonymous user base and the nature of the files that are shared. Such networks can lead accidental or deliberate release as well as malicious corruption, alteration, or deletion of information. File-sharing software may pose a threat to USAID data and information resources. (**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.

(**Chapter 545** and **557**)

**Freeware**
Freeware is defined as free software. Freeware, unlike shareware, such software is largely uncontrolled and proprietary (not subject to source review), and as a result might contain malicious code. (**Chapter 545**)

**Functional or Program Managers (PMs)**
A subclass of users, in some cases this role may require elevated privileges, including responsibilities for a daily program and operational management of their specific USAID system (including the USAID network). **(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**)

**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 who have no vested interest 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 Owner (IO)/Steward**
An Agency official that has been given 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). (**Chapter 545**)

**Information Security Vulnerability Management (ISVM)**
The cyclical practice of identifying, classifying, remediating, and mitigating information security vulnerabilities. (**Chapter 545**)

**Information System**
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)**
A. Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Agency; where B. such services or equipment are 'used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or three equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product. C. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources. D. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment. (**Chapter 545**)

**Information technology resource** includes all: A. Agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology; B. Acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but C. Does not include grants to third parties which establish or support information technology not operated directly by the Federal Government.” (**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 authority 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**)

**interconnection**
A connection between information systems. (**Chapter 545**)

**issue-specific policies**
These policies address specific areas of relevance and concern to the Agency (i.e., email, 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**)

**Memorandum of Understanding (MOU)**
A signed, non-obligating, and legally non-binding document that expresses the intent of IA and other participants (organizations) to connect IT systems, networks, and data for the mutual benefit of participants. An MOU focuses on participant roles and responsibilities in the development, management, operation, and security in the connection of IT resources. (**Chapter 545**)

**Mobile Computing Device (MCD)**
A small, handheld computing device, typically having a display screen with touch input or a miniature keyboard and weighing less than two 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. (**Chapter 502** and **545**)

**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**)

**National Security Information (NSI) System**
NSI is classified information. An NSI system is any system (i.e., network, end point, server, etc.) that is used to handle or process NSI information. Associated workspaces are areas where NSI exists. (**Chapter 545**)

**need to know**
The need for specific information not normally available without justification and

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**)

**open-source software**
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 nature of said software can pose a threat to USAID networks. (**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 U.S. 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 handheld device that provides computing and information storage and retrieval capabilities. A PDA is a Mobile Computing Device (MCD). (**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**)

**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 email address. PII can also consist of a combination of indirect data elements such as gender, race, birthdate, geographic indicator (i.e., zip code), and other descriptors used to identify specific individuals. Same as "information in an identifiable form". (**Chapter 508** and **545**)

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

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

**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**)

**portable media**
Portable storage devices (USB memory sticks, compact disks, digital video disks, external/removable hard disk drives), mobile devices with storage capability (smart phones, tablets, E-readers), and portable end points (laptops and netbooks). (**Chapter 545**)

**Privacy Act of 1974**
A Federal Law that governs the use, collection, maintenance and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. (**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. (**Chapter 508** and **545**)

**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 or SORN is required. (**Chapter 508** and **545**)

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

**program management**
Used in the context of this document, 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 (i.e., 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**)

**recovery point objective (RPO)**
The maximum targeted period in which data might be lost from an IT service due to a major incident. The RPO gives systems designers a limit to work to. (**Chapter 545**)

**recovery time objective (RTO)**
The targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. (**Chapter 545**)

**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. (**Chapter 545**)

**restricted authority to operate (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)**
Department of State, Bureau of Diplomatic Security Special Agents. They are responsible to the Chief of Mission at U.S. 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 access**
Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (i.e., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. (Source: **NIST SP 800-53 rev. 4**) (**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 executive**
An individual or group within the Agency that helps to ensure that risk-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. (**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**)

**security-related parameters**
Parameters affecting the security state of information systems including the parameters required to satisfy other security control requirements. They include registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections. (**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: 1) carrying out the CIO security responsibilities under FISMA; and 2) 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: 1) possesses professional qualifications, including training and experience, required to administer the information security program functions; 2) maintains information security duties as a primary responsibility; and 3) 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 or more individuals are needed to complete a process. This ensures that no single individual has complete control over process execution. (**Chapter 545**)

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

**Service Level Agreement**
A management agreement between USAID and a service provider. An SLA is a signed, obligating, and legally binding document that describes the services and products the service provider will provide to USAID pursuant to the contract. (**Chapter 545**)

**shareware**
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. (**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**)

**site**
"A site is the total computing environment that automated ISs, networks, or components operate. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other ISs." (From *DON DIACAP Handbook*, v1.0, 15 July 2008) (**Chapter 545**)

**social media**
Sites on the Internet that contain mobile-based tools or applications used for sharing and discussing information. Social media is broken into three categories: 1) File Sharing/Storage, 2) Social Networking and 3) Web Publishing. (**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 USC § 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)**
A subclass of users that require 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. Typically responsible for the technical security, installation, configuration, and maintenance of both the software and associated hardware and have elevated system privileges. In ADS 545, all personnel with elevated privileges are considered to be system administrators. (**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. (**Chapter 405** and **545**)

**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 Web sites. (**Chapter 545**)

**third-party**
The term refers to any non-Agency staff. (**Chapter 545**)

**third-party system**
An IT system that is external to a system. (**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, 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** and **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 back doors on federal systems, giving them access to 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**)

**type accreditation**
“In some situations, a system consisting of a common set of hardware, software, and firmware is intended for installation at multiple locations. A type accreditation satisfies the C&A requirements in this case by obtaining a single accreditation that permits installation of multiple instances of this specifically configured system in a particular physical/operational environment at multiple locations. Rather than testing and validating the system at every site where it is needed, the type accreditations allow for the installation of identical systems based on the validation of all the IACs at one representative site.” (Source: *DON DIACAP Handbook*, v1.0, 15 July 2008) (**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. (**Chapter 545** and **552**)

**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 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**
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. 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. Users are the only subclass that cannot possess elevated privileges. (**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, i.e., 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 back doors, 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**)

**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**)

**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**)

**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**)

545_101017