ADS Chapter 545

Information Systems Security

Partial Revision Date: 03/28/2023
Responsible Office: M/CIO/IA
File Name: 545_032823

Functional Series 500 – Management Services
ADS 545 – Information Systems Security
POC for ADS 545: See ADS 501maa, ADS Chapters and Point of Contact List

Table of Contents

545.1	**OVERVIEW**	**9**
545.2	**PRIMARY RESPONSIBILITIES**	**10**
545.3	**POLICY DIRECTIVES AND REQUIRED PROCEDURES**	**13**
545.3.1	**Program Management (PM)**	**14**
545.3.1.1	Information Security Program Plan (PM-1)	14
545.3.1.2	Information Security Program Leadership Role (PM-2)	14
545.3.1.3	Information Security and Privacy Resources (PM-3)	15
545.3.1.4	Plan of Action and Milestones Process (PM-4)	15
545.3.1.5	System Inventory (PM-5)	16
545.3.1.6	Measures of Performance (PM-6)	16
545.3.1.7	Enterprise Architecture (PM-7)	16
545.3.1.8	Critical Infrastructure Plan (PM-8)	17
545.3.1.9	Risk Management Strategy (PM-9)	17
545.3.1.10	Authorization Process (PM-10)	17
545.3.1.11	Mission and Business Process Definition (PM-11)	18
545.3.1.12	Insider Threat Program (PM-12)	18
545.3.1.13	Security and Privacy Workforce (PM-13)	18
545.3.1.14	Testing, Training, and Monitoring (PM-14)	18
545.3.1.15	Security and Privacy Groups and Associations (PM-15)	19
545.3.1.16	Threat Awareness Program (PM-16)	19
545.3.1.17	Protecting Controlled Unclassified Information on External Systems (PM-17)	19
545.3.1.18	Privacy Program Plan (PM-18)	20
545.3.1.19	Privacy Program Leadership Role (PM-19)	21
545.3.1.20	Dissemination of Privacy Program Information (PM-20)	21
545.3.1.21	Accounting of Disclosures (PM-21)	21
545.3.1.22	Personally Identifiable Information (PII) Quality Management (PM-22)	22
545.3.1.23	Data Governance Body (PM-23)	22
545.3.1.24	Data Integrity Board (PM-24)	22
545.3.1.25	Minimization of PII Used in Testing, Training, and Research (PM-25)	23
545.3.1.26	Complaint Management (PM-26)	23
545.3.1.27	Privacy Reporting (PM-27)	24
545.3.1.28	Risk Framing (PM-28)	24
545.3.1.29	Risk Management Program Leadership Roles (PM-29)	25
545.3.1.30	Supply Chain Risk Management (SCRM) Strategy (PM-30)	25

545.3.1.31 Continuous Monitoring Strategy (PM-31) 25
545.3.1.32 Purposing (PM-32) 26

545.3.2 Access Control (AC) 26
545.3.2.1 Policy and Procedures (AC-1) 26
545.3.2.2 Account Management (AC-2) 27
545.3.2.3 Access Enforcement (AC-3) 29
545.3.2.4 Information Flow Enforcement (AC-4) 29
545.3.2.5 Separation of Duties (AC-5) 30
545.3.2.6 Least Privilege (AC-6) 30
545.3.2.7 Unsuccessful Logon Attempts (AC-7) 31
545.3.2.8 System Use Notification (AC-8) 31
545.3.2.9 Device Lock and Session Termination (AC-11 and AC-12) 32
545.3.2.10 Permitted Actions Without Identification or Authentication (AC-14) 33
545.3.2.11 Remote Access (AC-17) 33
545.3.2.12 Wireless Access (AC-18) 34
545.3.2.13 Access Control for Mobile Devices (AC-19) 35
545.3.2.14 Use of External Systems (AC-20) 35
545.3.2.15 Information Sharing (AC-21) 36
545.3.2.16 Publicly Accessible Content (AC-22) 36

545.3.3 Awareness and Training (AT) 36
545.3.3.1 Policy and Procedures (AT-1) 37
545.3.3.2 Literacy Training and Awareness (AT-2) 37
545.3.3.3 Role-Based Training (AT-3) 39
545.3.3.4 Training Records (AT-4) 40

545.3.4 Audit and Accountability (AU) 40
545.3.4.1 Policy and Procedures (AU-1) 41
545.3.4.2 Event Logging (AU-2) 41
545.3.4.3 Content of Audit Records (AU-3) 42
545.3.4.4 Audit Log Storage Capacity (AU-4) 43
545.3.4.5 Response to Audit Logging Process Failures (AU-5) 43
545.3.4.6 Audit Record Review, Analysis, and Reporting (AU-6) 43
545.3.4.7 Audit Record Reduction and Report Generation (AU-7) 44
545.3.4.8 Time Stamps (AU-8) 44
545.3.4.9 Protection of Audit Information (AU-9) 45
545.3.4.10 Audit Record Retention (AU-11) 45
545.3.4.11 Audit Record Generation (AU-12) 45

545.3.5 Assessment, Authorization, and Monitoring (CA) 46
545.3.5.1 Policy and Procedures (CA-1) 46
545.3.5.2 Control Assessments (CA-2) 46
545.3.5.3 Information Exchange (CA-3) and Internal System Connections (CA-9) 47
545.3.5.4 Plan of Actions and Milestones (CA-5) 48
545.3.5.5 Authorization (CA-6) 49
545.3.5.6 Continuous Monitoring (CA-7) 50

545.3.6 Configuration Management (CM) 51
545.3.6.1 Policies and Procedures (CM-1) 52
545.3.6.2 Baseline Configuration (CM-2) 52
545.3.6.3 Configuration Change Control (CM-3) 53
545.3.6.4 Impact Analyses (CM-4) 53
545.3.6.5 Access Restrictions for Change (CM-5) 54
545.3.6.6 Configuration Settings (CM-6) 54
545.3.6.7 Least Functionality (CM-7) 54
545.3.6.8 System Component Inventory (CM-8) 55
545.3.6.9 Configuration Management Plan (CM-9) 56
545.3.6.10 Software Usage Restrictions (CM-10) 56
545.3.6.11 User-Installed Software (CM-11) 57
545.3.6.12 Information Location (CM-12) 57

545.3.7 Contingency Planning (CP) 58
545.3.7.1 Policy and Procedures (CP-1) 58
545.3.7.2 Contingency Plan (CP-2) 58
545.3.7.3 Contingency Training (CP-3) 59
545.3.7.4 Contingency Plan Testing (CP-4) 60
545.3.7.5 Alternate Storage Site (CP-6) 60
545.3.7.6 Alternate Processing Site (CP-7) 61
545.3.7.7 Telecommunications Services (CP-8) 62
545.3.7.8 System Backup (CP-9) 62
545.3.7.9 System Recovery and Reconstitution (CP-10) 63

545.3.8 Identification and Authentication (IA) 63
545.3.8.1 Policy and Procedures (IA-1) 63
545.3.8.2 Identification and Authentication (Organizational Users) (IA-2) 64
545.3.8.3 Device Identification and Authentication (IA-3) 64
545.3.8.4 Identifier Management (IA-4) 65
545.3.8.5 Authenticator Management (IA-5) 65
545.3.8.6 Authentication Feedback (IA-6) 68
545.3.8.7 Cryptographic Module Authentication (IA-7) 68
545.3.8.8 Identification and Authentication (Non-Organizational Users) (IA-8) 68
545.3.8.9 Digital Signature Using Personal Identity Verification (PIV) Card 69
545.3.8.10 Re-Authentication (IA-11) 69
545.3.8.11 Identity Proofing (IA-12) 70

545.3.9 Incident Response (IR) 70
545.3.9.1 Policy and Procedures (IR-1) 71
545.3.9.2 Incident Response Training (IR-2) 71
545.3.9.3 Incident Response Testing (IR-3) 71
545.3.9.4 Incident Handling (IR-4) / Incident Monitoring (IR-5) 72
545.3.9.5 Incident Reporting (IR-6) / Incident Response Assistance (IR-7) 72
545.3.9.6 Incident Response Plan (IR-8) 73
545.3.9.7 Information Spillage Response (IR-9) 74

545.3.10 Maintenance (MA) 75
545.3.10.1 Policy and Procedures (MA-1) 75
545.3.10.2 Controlled Maintenance (MA-2) 76
545.3.10.3 Maintenance Tools (MA-3) 76
545.3.10.4 Non-Local Maintenance (MA-4) 77
545.3.10.5 Maintenance Personnel (MA-5) 77
545.3.10.6 Timely Maintenance (MA-6) 78

545.3.11 Media Protection (MP) 78
545.3.11.1 Policy and Procedures (MP-1) 78
545.3.11.2 Media Access (MP-2) 79
545.3.11.3 Media Marking (MP-3) 79
545.3.11.4 Media Storage (MP-4) 79
545.3.11.5 Media Transport (MP-5) 80
545.3.11.6 Media Sanitization (MP-6) 80
545.3.11.7 Media Use (MP-7) 81
545.3.11.8 Media Downgrading (MP-8) 81

545.3.12 Physical and Environmental Protection (PE) 82
545.3.12.1 Policy and Procedures (PE-1) 82
545.3.12.2 Physical Access Authorizations (PE-2) 83
545.3.12.3 Physical Access Control (PE-3) and Visitor Access Records (PE-8) 83
545.3.12.4 Access Control for Output Devices (PE-5) 84
545.3.12.5 Monitoring Physical Access (PE-6) 84
545.3.12.6 Access Control for Transmission (PE-4) and Power Equipment and Cabling (PE-9) 84
545.3.12.7 Emergency Shutoff, Power and Lighting (PE-10, 11, 12) 85
545.3.12.8 Fire Protection (PE-13) 85
545.3.12.9 Environmental Controls (PE-14) 85
545.3.12.10 Water Damage Protection (PE-15) 85
545.3.12.11 Delivery and Removal (PE-16) 86
545.3.12.12 Alternate Work Site (PE-17) 86

545.3.13 Planning (PL) 86
545.3.13.1 Policy and Procedures (PL-1) 86
545.3.13.2 System Security and Privacy Plans (PL-2) 87
545.3.13.3 Rules of Behavior (ROB) (PL-4) 88
545.3.13.4 Security and Privacy Architectures (PL-8) 89
545.3.13.5 Central Management (PL-9) 90
545.3.13.6 Baseline Selection (PL-10) 90
545.3.13.7 Baseline Tailoring (PL-11) 90

545.3.14 Personnel Security (PS) 90
545.3.14.1 Policy and Procedures (PS-1) 91
545.3.14.2 Position Risk Designation (PS-2) 91
545.3.14.3 Personnel Screening (PS-3) 92

545.3.14.4 Personnel Termination (PS-4) 92
545.3.14.5 Personnel Transfer (PS-5) 92
545.3.14.6 Access Agreements (PS-6) 92
545.3.14.7 External Personnel Security (PS-7) 93
545.3.14.8 Personnel Sanctions (PS-8) 93
545.3.14.9 Position Descriptions (PS-9) 94

545.3.15 Personally Identifiable Information Processing and Transparency (PT) 94
545.3.15.1 Policy and Procedures (PT-1) 94
545.3.15.2 Authority to Process Personally Identifiable Information (PT-2) 95
545.3.15.3 Personally Identifiable Information Processing Purposes (PT-3) 95
545.3.15.4 Consent (PT-4) 95
545.3.15.5 Privacy Notice (PT-5) 96
545.3.15.6 System of Records Notice (PT-6) 96
545.3.15.7 Specific Categories of Personally Identifiable Information (PT-7) 97
545.3.15.8 Computer Matching Requirements (PT-8) 97

545.3.16 Risk Assessment (RA) 98
545.3.16.1 Policy and Procedure (RA-1) 98
545.3.16.2 Security Categorization (RA-2) 98
545.3.16.3 Risk Assessment (RA-3) 99
545.3.16.4 Vulnerability Management and Scanning (RA-5) 100
545.3.16.5 Risk Response (RA-7) 101
545.3.16.6 Privacy Impact Assessments (RA-8) 102
545.3.16.7 Criticality Analysis (RA-9) 102

545.3.17 System and Services Acquisition (SA) 102
545.3.17.1 Policy and Procedures (SA-1) 103
545.3.17.2 Allocation of Resources (SA-2) 103
545.3.17.3 System Development Life Cycle (SA-3) 104
545.3.17.4 Acquisition Process (SA-4) 104
545.3.17.5 System Documentation (SA-5) 106
545.3.17.6 Security and Privacy Engineering Principles (SA-8) 107
545.3.17.7 External System Services (SA-9) 108
545.3.17.8 Developer Configuration Management (SA-10) 109
545.3.17.9 Developer Testing and Evaluation (SA-11) 109
545.3.17.10 Development Process, Standards, and Tools (SA-15) 110
545.3.17.11 Unsupported System Components (SA-22) 111

545.3.18 System and Communications Protection (SC) 111
545.3.18.1 Policy and Procedures (SC-1) 111
545.3.18.2 Separation of System and User Functionality (SC-2) 112
545.3.18.3 Information in Shared System Resources (SC-4) 112
545.3.18.4 Denial-of-Service Protection (SC-5) 112
545.3.18.5 Boundary Protection (SC-7) 113
545.3.18.6 Transmission Confidentiality and Integrity (SC-8) 114

545.3.18.7 Network Disconnect (SC-10) 114
545.3.18.8 Cryptographic Key Establishment and Management (SC-12) 114
545.3.18.9 Cryptographic Protection (SC-13) 114
545.3.18.10 Collaborative Computing Devices and Applications (SC-15) 114
545.3.18.11 Public Key Infrastructure Certificates (SC-17) 115
545.3.18.12 Mobile Code (SC-18) 115
545.3.18.13 Secure Name/Address Resolution Service (Authoritative Source) (SC-20) 115
545.3.18.14 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21) 115
545.3.18.15 Architecture and Provisioning for Name/Address Resolution Service (SC-22) 116
545.3.18.16 Session Authenticity (SC-23) 116
545.3.18.17 Protection of Information at Rest (SC-28) 116
545.3.18.18 Process Isolation (SC-39) 116

545.3.19 System and Information Integrity (SI) 116
545.3.19.1 Policy and Procedures (SI-1) 117
545.3.19.2 Flaw Remediation (SI-2) 117
545.3.19.3 Malicious Code Protection (SI-3) 118
545.3.19.4 System Monitoring (SI-4) 119
545.3.19.5 Security Alerts, Advisories, and Directives (SI-5) 120
545.3.19.6 Software, Firmware, and Information Integrity (SI-7) 120
545.3.19.7 Spam Protection (SI-8) 120
545.3.19.8 Information Input Validation (SI-10) 121
545.3.19.9 Error Handling (SI-11) 121
545.3.19.10 Information Management and Retention (SI-12) 121
545.3.19.11 Memory Protection (SI-16) 121
545.3.19.12 Personally Identifiable Information Quality Operations (SI-18) 122
545.3.19.13 De-identification (SI-19) 122

545.3.20 Supply Chain Risk Management (SR) 122
545.3.20.1 Policy and Procedures (SR-1) 122
545.3.20.2 Supply Chain Risk Management Plan (SR-2) 123
545.3.20.3 Supply Chain Controls and Processes (SR-3) 124
545.3.20.4 Acquisition Strategies, Tools, and Methods (SR-5) 124
545.3.20.5 Supplier Assessments and Reviews (SR-6) 125
545.3.20.6 Notification Agreements (SR-8) 125
545.3.20.7 Inspection of Systems and Components (SR-10) 125
545.3.20.8 Component Authenticity (SR-11) 125
545.3.20.9 Component Disposal (SR-12) 125

545.3.21 Other USAID-Specific Policies 126
545.3.21.1 Acceptable Use 126
545.3.21.2 Information Security Policy Violation and Disciplinary Action 128
545.3.21.3 Requirement to Connect Laptops to AIDNet Every 30 Days 128
545.3.21.4 Elevated Privilege Account Usage Limitations 129

545.3.22 Prohibited and Restricted Use Technologies 129
545.3.22.1 Social Media and Social Networking 129

545.3.23 Other Technologies 131
545.3.23.1 Third-Party Websites 131
545.3.23.2 Cloud Computing 132
545.3.23.3 Applications or Services Sending Emails Using USAID.gov Email Address 133

545.3.24 Waivers 133

545.4 MANDATORY REFERENCES 134

545.4.1 External Mandatory References 134

545.4.2 Internal Mandatory References 137

545.5 ADDITIONAL HELP 138

545.6 DEFINITIONS 138

ADS 545 – Information Systems Security

545.1 OVERVIEW

Effective Date: 03/28/2023

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 that support the operations and assets of the agency, including those provided or managed by another agency or contractor on USAID's behalf. 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 the entire USAID workforce and IT services, systems, 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 systems. This includes, but is not limited to, United States Direct-Hires (USDHs), Personal Services Contractors (PSCs), Fellows, Participating Agency Service Agreement (PASA), and contractor personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS Chapter 501, The Automated Directives System**. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to **Homeland Security Presidential Directive 12 (HSPD-12)** and information security requirements.

The standards established in this chapter represent the minimum standards for information systems security for a USAID system with a risk categorization of Moderate impact, in accordance with **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5**. However, when a system is categorized as Low or High for security impact, these standards will be tailored in accordance with minimum security and privacy controls, as defined by NIST SP 800-53, Revision 5, for the specific security categorization.

USAID must comply with **Binding Operational Directives (BODs) and Emergency Directives (EDs)**, issued by the U.S. Department of Homeland Security (DHS).

USAID must comply with cybersecurity **memoranda** that address cybersecurity requirements or implementation guidance for Executive Agencies issued by the Office of Management and Budget (OMB).

Refer to **ADS 552, Cyber Security for National Security Information (NSI) Systems** for compliance requirements for classified systems.

Any specific responsibilities for risk management mentioned in this chapter will be exercised consistent with the Agency Enterprise Risk Management governance structure detailed in **ADS 596mab, Governance Charter for Enterprise Risk Management and Internal Control at USAID**.

545.2 PRIMARY RESPONSIBILITIES

Effective Date: 12/28/2022

All federal agencies and the USAID workforce bear primary responsibilities for information systems security. Although contractors, PSCs, and others working on behalf of USAID may support security functions, a USDH must always be designated as the owner of a system, e.g. the responsible person who ensures that all security controls are implemented.

a. The **Administrator (A/AID)** is, pursuant to FISMA, 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 Agency;

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

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

4. Fulfills this responsibility by delegating to the Chief Information Officer the authority to ensure compliance with FISMA.

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 Office of the CIO to USAID's Authorizing Official (AO), Information System Owners (SOs), common control providers, and Information System Security Officers (ISSOs). The CISO (or supporting

workforce 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 it complies with all applicable statutory and regulatory guidance. 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 **Chief Data Officer (CDO)** protects the Agency's data, data quality, and data lifecycle management. The CDO also identifies ways for the Agency to better use and make its data accessible to the public, as appropriate. The CDO chairs the USAID Data Administration and Technical Advisory (DATA) Board and serves on the Agency's Privacy Council.

f. 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. At USAID, the CIO is the SAORM.

g. The **Senior Accountable Official for Supply Chain Risk Management (SAO-SCRM)** manages the Agency's Information and Communications Technology (ICT) Supply Chain. At USAID, the CIO is the SAO-SCRM.

h. The **Senior Agency Official for Privacy (SAOP)** has overall responsibility and accountability for fulfilling the requirements of OMB M-16-24. This necessitates working with the CPO to ensure the Agency's implementation of information privacy protections and Agency compliance efforts. These responsibilities include pursuing 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 the Office of Management and Budget (OMB)/ DHS reporting requirements. The SAOP is also responsible for ensuring that all members of the workforce receive the appropriate privacy training, both annual and role-based. The SAOP works with the CPO to carry out this responsibility.

i. 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 IO of the information processed, stored, or transmitted by an information system may or may not be the same as the SO.

j. The **Business Owner (BO)** has varying responsibilities depending on the mission, business, or IO. In general, BOs are responsible for ensuring the mission of the organization is accomplished. In some cases, BOs are responsible for funding and other resources that support their line of business.

k. The **Authorizing Official (AO)** is the 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. At USAID, the CIO is the AO for information systems. Only the AO may officially accept information system risks on behalf of the Agency. The AO may deny authorization to operate an information system or, if the system is operational, halt operations if unacceptable risks exist.

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

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; and

4) Remediating weaknesses identified for associated common controls.

m. 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. The 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 ISSO, the 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 and privacy controls. In coordination with the IO, the 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 the Rules of Behavior (ROB).

The roles of SO and ISSO are separate and must be separately designated and assigned for the Missions and systems across the Agency. The roles may not be held by the same person. The Bureau for Management, Office of the Chief Information Office (M/CIO) provides training to SOs and ISSOs.

n. The **Information System Security Officer (ISSO)** ensures that the appropriate operational security posture is maintained for an information system and, as such, works in close collaboration with the SO and other related system Points of Contacts (POCs), including developers, engineers, and administrators. 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 is assigned responsibility for the day-to-day security operations of a system. The ISSO may be a non-USDH staff member but must be a U.S. citizen with a clearance at least equal to the highest security classification of the information being protected.

o. The **Information Security Architect** ensures 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 systems supporting those missions and business processes.

p. The **Information System Security Engineer** conducts 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** conducts 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 and deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. The assessor must document the results of the assessment in a security assessment report.

545.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 12/28/2022

This chapter defines the Agency's information security policy and is used to measure progress and compliance. The CISO maintains this policy and may alter it to comply with Federal regulations, mandates, and directives by way of periodic updates and/or Agency Notices, as required, to maintain the security of the Agency's information security profile.

At the discretion of the A/AID, or designees, certain USAID security authorization roles may be delegated (*i.e.,* role representatives). Delegations must follow ADS 103 and documented consistent with ADS 103. When roles and responsibilities in this chapter are delegated, those delegations should be recorded in the office of the delegator and

delegee for ready access by the agency. Bureau/Independent Office/Mission (B/IO/M) officials may appoint qualified individuals to perform activities associated with any USAID security authorization role, with the exception of the CIO, CISO, CPO, and AO.

Please note: Sections **545.3.1** through **545.3.20** correspond to required security and privacy controls, per **NIST 800-53, Rev. 5**. The abbreviation following each section heading includes the identifier for that control (*e.g.,* PM for Program Management, AC for Access Control, AT for Awareness and Training, etc.).

545.3.1 Program Management (PM)

Effective Date: 12/28/2022

The PM control family covers the high-level management and operations of the Agency's cybersecurity program, promoting a comprehensive management approach across all USAID information systems.

545.3.1.1 Information Security Program Plan (PM-1)

Effective Date: 12/28/2022

The CISO must develop, document, disseminate, protect, review annually, and update as required, an Agency-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 that are 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 the A/AID through the Agency Executive Management Council on Risk and Internal Control (EMCRIC) considering the risk being incurred to USAID operations (including mission, functions, image, and reputation), USAID assets, and individuals (see **ADS 596, Management's Responsibility for Internal Control**).

545.3.1.2 Information Security Program Leadership Role (PM-2)

Effective Date: 12/28/2022

The CIO, or designee, must appoint an experienced senior information security officer or CISO with the mission and resources to coordinate, develop, implement, and maintain a USAID-wide Information Security Program.

545.3.1.3 Information Security and Privacy Resources (PM-3)
Effective Date: 12/28/2022

The Agency must:

a. Ensure that all capital planning and investment requests include the resources needed to implement the information security and privacy programs and document 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.

b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards; and

c. Make available for expenditure, the planned information security and privacy resources.

SOs, BOs, the AO, and the SAOP are responsible for ensuring these requirements are met for all IT assets deployed for Agency operations. For details, see **ADS 509, Management and Oversight of Agency Information Technology Resources**; **ADS 547, Property Management of Information Technology (IT)**; **ADS 562, Physical Security Programs (Overseas)**; and **OMB Cyber Spend Reporting Requirements/Budget Data Requests (BDR)**.

545.3.1.4 Plan of Action and Milestones Process (PM-4)
Effective Date: 12/28/2022

The CISO must:

a. Implement a process for ensuring that POA&Ms for the security, privacy, and SCRM programs and associated organizational information systems are developed and maintained;

b. Document the remedial information security, privacy, and SCRM 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 POA&Ms for consistency with the organizational risk management strategy and Agency-wide priorities for risk response actions.

For more information, please see the **POA&M Management Guide for Documenting Weakness**. To obtain a copy of this document, go to the **Security and Assessment Authorization (SA&A) Process** page.

545.3.1.5 System Inventory (PM-5)
Effective Date: 12/28/2022

M/CIO must:

a. Develop, maintain, and update at least monthly an inventory of Agency information systems, including approved social media sites and cloud-based systems/services.

b. Establish, maintain, and update annually, or more frequently as required, an inventory of all systems, applications, and projects that process PII to ensure that they only process the PII for an authorized purpose and that this processing is still relevant and necessary for the specified purpose.

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.

SOs, with assistance from their ISSOs, must maintain an inventory of all hardware, software, and service assets associated with their systems.

545.3.1.6 Measures of Performance (PM-6)
Effective Date: 12/28/2022

The CISO must develop, monitor, and report the results of information security and privacy measures of performance as part of the Agency Information Security and Privacy Programs. Reporting must include outcome-based metrics demonstrating the effectiveness of the security and privacy 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: 12/28/2022

M/CIO must develop and maintain an enterprise architecture integrated with information security and privacy at an Agency-wide level. The security and privacy controls within the enterprise architecture must address risks to Agency individuals, assets, and operations while protecting Agency core missions and business processes and aligning with the Federal Enterprise Architecture to protect other organizations and the Nation.

M/CIO must consider, when feasible, moving supportive but non-essential functions to a non-critical system, system component, or external provider to gain efficiencies and reduce the attack surface of the USAID enterprise.

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: 12/28/2022

If the A/AID officially declares that the Agency mission includes critical infrastructure, M/CIO 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 and privacy issues when developing, documenting, and updating the critical infrastructure. This includes the creation of a key resources protection plan.

545.3.1.9 Risk Management Strategy (PM-9)

Effective Date: 12/28/2022

M/CIO must develop, implement, review annually, and update as required, an Agency-wide risk management strategy to manage security and privacy risk to organizational operations and assets, individuals, other organizations, and the Nation. M/CIO must provide sufficient resources to implement the risk management strategy. An Agency-wide risk management strategy must include, at a minimum:

- Expression of the security and privacy risk tolerance for the Agency (see **ADS 596**);
- Acceptable risk assessment methodologies;
- Security and privacy risk mitigation strategies;
- Consistent implementation of the risk management strategy across the Agency; and
- A review schedule to address organizational updates or changes.

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

545.3.1.10 Authorization Process (PM-10)

Effective Date: 12/28/2022

The CISO must develop, implement, and manage an Agency-wide security authorization process which tests the effectiveness of security and privacy controls and integrates with the Agency's risk management program and continuous monitoring processes. 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 (GSS), including cloud-based systems, and serve as the primary contact for all security matters.

For details, see **NIST SP 800-37** and the **IT Systems Accreditation Risk Management Framework (RMF) Handbook** (available on the **SA&A Process** page).

545.3.1.11 Mission and Business Process Definition (PM-11)
Effective Date: 12/28/2022

BOs, in coordination with M/CIO, must:

a. Define Agency mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, assets, individuals, other organizations, and the Nation;

b. Determine information protection and PII processing needs arising from the defined mission and business processes; and

c. Review and revise the mission and business processes annually or more frequently, as necessary.

545.3.1.12 Insider Threat Program (PM-12)
Effective Date: 12/28/2022

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, including a cross-discipline insider threat incident handling team. The program must provide policies, implementation plans, and monitoring of workforce activities on government-owned systems, as well as training to employees. The Agency must ensure SEC, CISO, and other offices as necessary receive access to information, such as personnel records, to support analysis of potential insider threats and to conduct self-assessments of the insider threat posture. 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 and Insider Threat Program** and **E.O. 13587**.

545.3.1.13 Security and Privacy Workforce (PM-13)
Effective Date: 12/28/2022

The CISO, in coordination with M/CIO and the Office of Human Capital and Talent Management (HCTM), must establish an information security and privacy workforce development and improvement program to institutionalize core information security and privacy capabilities. This includes defining knowledge, skills, and abilities needed by the information security and privacy workforce, conducting role-based training for them, and providing standards and guidelines to measure and build individual qualifications for incumbents and applicants for security and privacy positions.

545.3.1.14 Testing, Training, and Monitoring (PM-14)
Effective Date: 12/28/2022

The CISO must:

- Develop, implement, and maintain an Agency-wide process to execute timely security and privacy testing, training, and monitoring;

- Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and Agency-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 800-37**, **NIST SP 800-53A**, and **NIST SP 800-137**.

545.3.1.15 Security and Privacy Groups and Associations (PM-15)

Effective Date: 12/28/2022

The CISO, and their designees, must establish and institutionalize contact with selected external security and privacy communities. The purpose of this contact is to:

- Facilitate ongoing security and privacy education and training for the USAID workforce;

- Maintain currency with recommended security and privacy practices, techniques, and technologies; and

- Share current security and privacy information regarding threats, vulnerabilities, incidents, tools, and techniques in compliance with appliable laws, Executive Orders, directives, policies, regulations, standards, and guidelines to safeguard Agency assets and operations.

545.3.1.16 Threat Awareness Program (PM-16)

Effective Date: 12/28/2022

The CISO must implement a threat awareness program that includes sharing threat information among general users, SOs, ISSOs, and their designees. Sharing information for purposes of threat awareness mitigates risks, including Advanced Persistent Threat (APT), to Agency assets and operations. Shared information can cover 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. The CISO must employ automated mechanisms to maximize the effectiveness of sharing threat information by providing the ability to rapidly share and feed relevant threat detection signatures into monitoring tools.

545.3.1.17 Protecting Controlled Unclassified Information on External Systems (PM-17)

Effective Date: 12/28/2022

The CISO must:

a. In collaboration with SEC, establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems are implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards; and

b. Review and update the policy and procedures annually or more frequently, as required.

545.3.1.18 Privacy Program Plan (PM-18)

Effective Date: 12/28/2022

The SAOP, in conjunction with the CPO, must:

a. Develop and disseminate an Agency-wide privacy program plan. The privacy program plan must:

1. Include a description of the structure of the privacy program and the resources dedicated to the privacy program;

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

3. Include the role of the SAOP and identify and assign roles and responsibilities for other privacy officials and members of the workforce;

4. Describe management commitment, compliance, and the strategic goals and objectives of the privacy program; and

5. Reflect coordination among Agency entities responsible for the different aspects of privacy.

b. Obtain approval for the plan from a senior official with responsibility and accountability for the privacy risk being incurred to Agency operations (including mission, functions, image, and reputation), Agency assets, individuals, other organizations, and the Nation.

c. Update the plan annually, or more frequently as necessary, to address changes in Federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

d. Designate the privacy controls the Agency will treat as program management, common, system-specific, and hybrid controls, and ensure the common controls

are documented in an appendix to the privacy program plan or in separate privacy plans for systems.

545.3.1.19 Privacy Program Leadership Role (PM-19)

Effective Date: 12/28/2022

The Agency must appoint an SAOP with the authority, mission, accountability, and resources to coordinate, develop, and implement applicable privacy requirements and manage privacy risks through the Agency-wide privacy program.

545.3.1.20 Dissemination of Privacy Program Information (PM-20)

Effective Date: 12/28/2022

The SAOP, in conjunction with the CPO, must:

a. Maintain a central resource webpage on the Agency's principal public website that:

1. Serves as a central source of information about the Agency's privacy program;

2. Ensures that the public has access to information about Agency privacy activities and can communicate with its SAOP;

3. Ensures that Agency privacy practices and reports are publicly available; and

4. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

b. Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:

1. Are written in plain language and organized in a way that is easy to understand and navigate;

2. Provide information needed by the public to make an informed decision about whether and how to interact with the Agency; and

3. Are updated whenever the Agency makes a substantive change to the practices described and includes a time/date stamp to inform the public of the date of the most recent changes.

545.3.1.21 Accounting of Disclosures (PM-21)

Effective Date: 12/28/2022

The SAOP, in conjunction with the CPO, must:

a. Develop and maintain an accurate accounting of disclosures of PII, including:

1) Date, nature, and purpose of each disclosure; and

2) Name and address, or other contact information of the individual or organization to which the disclosure was made.

b. Retain the accounting of disclosures for the length of the time the PII is maintained or five years after the disclosure is made, whichever is longer.

c. Make the accounting of disclosures available to the individual to whom the PII relates upon request.

545.3.1.22 Personally Identifiable Information (PII) Quality Management (PM-22)

Effective Date: 12/28/2022

The SAOP, in conjunction with the CPO, must develop and document Agency-wide policies and procedures for:

a. Reviewing the accuracy, relevance, timeliness, and completeness of PII across the information lifecycle which includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition of PII;

b. Correcting or deleting inaccurate or outdated PII;

c. Disseminating notice of corrected or deleted PII to individuals or other appropriate entities; and

d. Appeals of adverse decisions on correction or deletion requests.

545.3.1.23 Data Governance Body (PM-23)

Effective Date: 12/28/2022

The Agency must establish a Data Governance Body to serve as a central venue for seeking input from Agency stakeholders regarding data-related priorities and best practices to support Agency objectives. The USAID DATA Board serves in this capacity and informs data-related policies, procedures, and standards for the Agency. The DATA Board is chaired by the CDO with participation from the Evaluation Officer, Statistical Official, and Performance Improvement Officer, and relevant senior-level staff in Agency business units, data functions, and financial management (see **ADS 579**; **Foundations for Evidence-Based Policymaking Act of 2018** (Evidence Act); and subsequent guidance from OMB in Memoranda **M-19-18** and **M-19-23**).

545.3.1.24 Data Integrity Board (PM-24)

Effective Date: 12/28/2022

The Agency must establish a Data Integrity Board to:

a. Review proposals to conduct or participate in a matching program; and

b. Conduct an annual review of all matching programs in which the Agency has participated.

For the purposes of this section and as necessary, USAID's Privacy Council serves as a Data Integrity Board and consists of the following permanent members (or designated representatives):

- SAOP;
- CPO;
- CDO; and
- Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD) Division Chief.

Ad hoc members will include representatives from affected Bureaus or Offices as determined by the board (see **ADS 508** and **ADS 579** for more information).

545.3.1.25 Minimization of PII Used in Testing, Training, and Research (PM-25)

Effective Date: 12/28/2022

The Agency must:

a. Develop, document, and implement policies and procedures that address the use of PII for internal testing, training, and research;

b. Limit or minimize the amount of PII used for internal testing, training, and research purposes;

c. Authorize the use of PII when such information is required for internal testing, training, and research; and

d. Ensure the SAOP, CPO, and CDO review and update PII policies and procedures annually or more frequently, as necessary.

See **ADS 508** and **ADS 579** for more information.

545.3.1.26 Complaint Management (PM-26)

Effective Date: 12/28/2022

The SAOP in conjunction with the CPO must implement a process for receiving and responding to complaints, concerns, or questions from individuals about the Agency's

security and privacy practices that includes:

a. Mechanisms that are easy to use and readily accessible by the public;

b. All information necessary for successfully filing complaints;

c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within 20 working days;

d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within five working days, when possible; and

e. Response to complaints, concerns, or questions from individuals within 20 working days.

545.3.1.27 Privacy Reporting (PM-27)

Effective Date: 12/28/2022

The SAOP in conjunction with the CPO must:

a. Develop privacy reports and disseminate to:

1) OMB, Congress, and other oversight bodies, as appropriate, to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and

2) Senior Agency management and other personnel with responsibility for monitoring privacy program compliance.

b. Review and update privacy reports, as necessary.

545.3.1.28 Risk Framing (PM-28)

Effective Date: 12/28/2022

The CIO must:

a. Identify and document:

1. Assumptions and constraints affecting risk assessments, risk responses, and risk monitoring;

2. Priorities and trade-offs considered by the Agency for managing risk; and

3. Agency risk tolerance.

b. Distribute the results of risk framing activities to the A/AID, through the EMCRIC.

c. Review and update risk framing considerations semi-annually or more frequently, as necessary.

See **ADS 596** for more information.

545.3.1.29 Risk Management Program Leadership Roles (PM-29)
Effective Date: 12/28/2022

The Agency must:

a. Appoint a SAORM to align Agency information security and privacy management processes with strategic, operational, and budgetary planning processes; and

b. Establish a Risk Executive (function) to view and analyze risk from an Agency-wide perspective and ensure management of risk is consistent across the Agency.

See **ADS 596** for more information.

545.3.1.30 Supply Chain Risk Management (SCRM) Strategy (PM-30)
Effective Date: 12/28/2022

The SAO-SCRM must:

a. Develop an Agency-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

b. Implement the SCRM strategy consistently across the Agency;

c. Review and update the supply chain risk management strategy semi-annually or more frequently as required, to address organizational changes; and

d. Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

See **Section 889(a)(1)(B)** of the **John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232)**.

545.3.1.31 Continuous Monitoring Strategy (PM-31)
Effective Date: 12/28/2022

The CISO must develop an Agency-wide continuous monitoring strategy and implement continuous monitoring programs that include the:

a. Establishment of Agency-wide metrics to be monitored in response to Inspector General (IG) FISMA metrics;

b. Establishment of monthly data collection for the purpose of monitoring, and annual assessments of control effectiveness;

c. Ongoing monitoring of Agency-defined metrics in accordance with the continuous monitoring strategy;

d. Correlation and analysis of information generated by control assessments and monitoring;

e. Response actions to address results of the analysis of control assessment and monitoring information; and

f. Reporting the security and privacy status of Agency systems to the CIO, SAOP, and AO following assessments.

545.3.1.32 Purposing (PM-32)
Effective Date: 12/28/2022

The CIO must, on an annual basis or more frequently as required, analyze Agency systems, components, and devices supporting Agency mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

In cases in which CIO determines that Agency IT resources are not being utilized for their intended purpose, CIO will, dependent on the risk to the Agency, take any of the following actions:

a. Through SOs and ISSOs, develop Plans of Action and Milestones (POA&Ms) to resolve the discrepancy in systems, components, or devices; or

b. Notify the SO that the system, component, or device will be decommissioned by a specific date and removed from the network if it is determined that the system, component, or device does not comply with USAID standards, or presents an unacceptable risk to the Agency.

545.3.2 Access Control (AC)
Effective Date: 12/28/2022

Access control is the restriction to Agency resources and information to only approved entities through authentication and authorization.

545.3.2.1 Policy and Procedures (AC-1)
Effective Date: 12/28/2022

The CISO must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency access control policy that:

1. Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Review the access control policy annually and update as needed.

c. Designate a policy lead to manage the development, documentation, and dissemination of the access control policy.

SOs must:

a. Develop, document, implement, and disseminate to users system-level procedures to facilitate the implementation of the access control policy and the associated access controls.

b. Review access control procedures at least annually and update as needed and following system security breaches, to comply with Agency policy and to protect resources from unauthorized alteration, loss, unavailability, or disclosure.

545.3.2.2 Account Management (AC-2)

Effective Date: 12/28/2022

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

- A valid access authorization;
- Intended system usage; and
- Other system-specific attributes as required by USAID or associated missions/business functions.

SOs must:

a. Support the management of system accounts using automated mechanisms.

b. Configure the system to automatically disable accounts when accounts:

1. Have expired,

2. Are no longer associated with a user or an individual,

3. Are in violation of Agency policy, or

4. Have been inactive for 90 days.

c. Disable accounts of individuals within 24 hours of discovery of security violations.

d. Assign an account manager (or group) for system 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. Require approvals by Contracting Officers (COs) or Contracting Officer's Representatives (CORs) for contractors to be included in group and role membership.

f. Specify:

1. Authorized users of the system;

2. Group and role membership; and

3. Access authorizations (*i.e.,* privileges) and other attributes (as required) for each account.

Note: Group or shared accounts/passwords include 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 chapter.

g. Establish and implement a process for changing shared or group account authenticator (if deployed) when individuals are removed from the group.

h. Configure the system to automatically audit account creation, modification, enabling, disabling, and removal actions.

i. Require that users log out at the end of the day or when absence for two hours is expected.

j. 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, file permissions, database object permissions, firewall rules, or user passwords.

k. Monitor the use of accounts.

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

m. Align account management processes with personnel termination and transfer processes.

n. Create, enable, modify, disable, and remove accounts in accordance with **ADS 502, The USAID Records Management Program** and the **ISSO Handbook** (available on the **SA&A Process** page).

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 30 days. The SO must suspend or disable accounts for users on extended absences. The SOs must establish a process to re-enable such accounts.

All SOs, IOs, and Bureaus must coordinate with ISSOs or M/CIO to establish a process to notify account managers within:

a. Five days when accounts are no longer required,

b. Three days when users are terminated or transferred, and

c. Three days when an individual's system usage or need-to-know changes.

545.3.2.3 Access Enforcement (AC-3)
Effective Date: 12/28/2022

SOs must configure the information system to enforce access with approved credential methods for logical access to information and system resources in accordance with **HSPD-12**, Identification and Authentication policies, and system-specific access policies.

545.3.2.4 Information Flow Enforcement (AC-4)
Effective Date: 12/28/2022

SOs must configure the system to enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on interconnection security agreements (ISAs), memorandums of understanding (MOUs),

memorandums of agreement (MOAs), and access control lists (ACLs) (see the **SA&A Process** page for a link to these and other System Development Life Cycle (SDLC) templates).

545.3.2.5 Separation of Duties (AC-5)

Effective Date: 12/28/2022

SOs must identify and document critical system functions among different individuals or groups and define system access authorizations to support separation of duties. This is documented through a Separation of Duties matrix (see the **SA&A Process** page for a link to this and other security artifact templates).

545.3.2.6 Least Privilege (AC-6)

Effective Date: 12/28/2022

SOs must:

a. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned USAID tasks.

b. Review quarterly the privileges assigned to Privileged Users to validate the need for such privileges, and reassign or remove privileges, if necessary, to correctly reflect USAID's mission and business needs.

c. Log the execution of privileged functions.

d. Prevent non-privileged users from executing privileged functions.

e. Authorize access for individuals to perform:

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.

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

g. Restrict privileged accounts on the system to approved and authorized system administrators.

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

545.3.2.7 Unsuccessful Logon Attempts (AC-7)

Effective Date: 12/28/2022

SOs must configure the 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 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 section **545.3.22.2**, Mobile Devices).

545.3.2.8 System Use Notification (AC-8)

Effective Date: 12/28/2022

SOs must configure the system to:

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

SECURITY / MONITORING STATEMENT

You are accessing a U.S. Government system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This system is provided for U.S. Government-authorized use only. The system usage may be monitored, recorded, and subject to audit.

M/CIO is responsible for compliance and enforcement of this policy and consistent with this authority, may take action necessary to prevent risk to USAID information or systems. Unauthorized or improper use of this system is prohibited and may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

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

Communications or data transiting or stored on this system may be disclosed or used for any lawful government purpose. Your consent is final and irrevocable. Other statements or informal policies inferring that you have an expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, are not enforceable, except when approved by the CIO.

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:

1. Display to users a system use information before granting further access to the publicly accessible system; and

2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

d. Include a description of the authorized uses of the system.

e. For the Agency's Continuous Diagnostics and Mitigation (CDM) Dashboard: display to users the CDM Program's model language, for log-on banners for computers, that is cleared by the Agency CDM POC.

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

Effective Date: 12/28/2022

A device 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 systems at the end of the day or when prolonged absences are expected.

SOs must configure the system to:

a. Initiate a device lock after 20 minutes of inactivity or when an end user manually initiates a device lock (*e.g.,* CTRL+ALT+DEL) before leaving the system unattended;

b. Ensure that end user devices lock after 20 minutes and application sessions terminate after 60 minutes of inactivity. For network session terminations, see section **545.3.18.7**, SC-10;

c. Retain the device lock until the user re-authenticates;

d. Conceal, via the device 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: 12/28/2022

SOs must:

a. Identify and approve read-only publicly releasable data, as approved by Legislative and Public Affairs (LPA), that can be performed on the system without identification or authentication consistent with organizational Missions/business functions; and

b. Document and provide supporting rationale regarding permitted user actions not requiring identification or authentication in the system security plan.

545.3.2.11 Remote Access (AC-17)
Effective Date: 12/28/2022

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

Remote access to USAID systems requires two-factor authentication. The mechanism must be approved by M/CIO. Currently, the only approved means are the **HSPD-12** Personal 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 140-3, Security Requirements for Cryptographic Modules**.

Remote access to SBU information, to include PII, must only be made using virtual desktop infrastructure (VDI), a virtual private network (VPN) or strong two-factor authentication using **FIPS 140-3** certified encryption to protect the information in transit as well as while at rest on a physical device. USAID employees are required to comply with **ADS 508** for proper handling and safeguarding of SBU and PII data. It is against Agency policy for employees to download PII to external storage devices (*i.e.,* USB drive) and non-GFE devices using remote access technologies, such as VDI or VPN. All downloads must follow the concept of least privilege, as documented in the SSP.

The SSP and Risk Assessment must document any remote access of PII and must be approved by the CPO prior to implementation. For more information regarding remote access of PII, see **ADS 508**. 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 each type of remote access to the system prior to allowing such connections;

c. Employ automated mechanisms 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 remote accesses through authorized and managed access control points (the number of managed access points is system specific); and

f. Explicitly authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides accessible evidence for all system administration except for security appliances and document the rationale for remote access in the security plan for the system.

The USAID workforce 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: 12/28/2022

SOs must:

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access;

b. Authorize each type of wireless access to the system prior to allowing such connections;

c. Protect wireless access to the system using approved encryption mechanisms and user-based authentication;

d. Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment;

e. 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

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

See **ADS 545mbg, Wireless Standards and Guidelines** and section **545.3.22.2**, Mobile Devices, for additional information.

545.3.2.13 Access Control for Mobile Devices (AC-19)

Effective Date: 12/28/2022

The Agency must:

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

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

SOs must:

1. Establish configuration requirements, connection requirements, and implementation guidance for USAID-controlled mobile devices, to include when such devices are outside of controlled areas;

2. Authorize the connection of mobile devices to organizational 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 Systems (AC-20)

Effective Date: 12/28/2022

SOs must establish terms and conditions and identify reasonable controls to be implemented on external systems for Agency work, consistent with the trust relationships established with other organizations owning, operating, or maintaining the external systems. The terms and conditions for using external systems, and the controls asserted to be implemented on external systems, must include the provisions for allowing authorized individuals to access the system from external information systems and process, store, or transmit USAID-controlled information using external systems. The use of Agency-controlled portable devices on external systems by authorized individuals are limited to the terms and conditions specified in access control agreements.

SOs must prohibit the use of Non-FedRAMP external or commercial systems for Agency work, unless the AO agrees in writing to accept the risk of using a specific Non-

FedRAMPed or commercial system. This control recognizes that there are circumstances where the USAID workforce using external systems (*i.e.,* contractors) need to access Agency systems.

AOs must only authorize the use of external systems to access the system or 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 the USAID Security Assessment and Authorization (SA&A) Process, documented in the **IT Systems Accreditation Risk Management Framework (RMF) Handbook** (available on the **SA&A Process** page). This must be specified in the SSP and in an approved system connection agreement or similar agreements with the organizational entity hosting the external system.

545.3.2.15 Information Sharing (AC-21)

Effective Date: 12/28/2022

The AO, in coordination with SOs, IOs, or BOs, must:

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for sensitive information, and

b. Employ automated mechanisms or manual processes to assist users in making information sharing and 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: 12/28/2022

SOs must:

a. Designate individuals authorized to make information publicly accessible;

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 system to ensure that non-public information is not included; and

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

545.3.3 Awareness and Training (AT)

Effective Date: 12/28/2022

Awareness and training of the USAID workforce are critical to ensuring the Agency's mission is accomplished. Each workforce member must be equipped with the knowledge and skills required to defend against constantly evolving threats to Agency assets and data. The scope of the AT section of this policy is limited to USAID workforce members who have logical access to the AIDNet information system. The AIDNet Information System is a General Support System (GSS), and scope is limited to those users to maintain reasonable efficiency and effectiveness for control of this AT policy. All AIDNet users have a usaid.gov email account.

545.3.3.1 Policy and Procedures (AT-1)

Effective Date: 12/28/2022

The CISO must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency security and privacy awareness and training policy applicable to users with logical AIDNet access to Active Directory (AD) accounts that:

1. Address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Are consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Develop procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls.

c. Designate a policy lead to manage the development, documentation, and dissemination of the awareness and training policy and procedures.

d. Review and update the policy and procedures annually or following changes from an assessment or audit finding, security or privacy incident, or changes in applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

The security and privacy awareness and training policy and program applies to all USAID workforce members.

545.3.3.2 Literacy Training and Awareness (AT-2)

Effective Date: 12/28/2022

The objectives of initial and annual general 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 and privacy practices within USAID.

a. The Agency must provide, and all workforce members must complete, security and privacy literacy training:

1. Initial Security and Privacy Literacy Training: All USAID workforce members must complete initial training in security and privacy awareness and accepted security and privacy practices.

Note: M/CIO and SEC will only accept USAID security training certificates; all new members of the workforce must complete USAID's initial security and privacy literacy training.

2. Annual Security and Privacy Awareness Training: All USAID workforce members with logical AIDNet access and AD accounts must complete annual refresher training in security and privacy awareness and accepted security and privacy practices.

Note: Security and privacy awareness training requirements cannot be waived or exempted for any USAID workforce member. In very 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. Failure to comply with the Annual Security and Privacy Awareness Training will result in the restriction or revocation of access to USAID networks, information systems, and resources.

b. The Agency employs the following techniques to increase the security and privacy awareness of workforce members:

- Administers initial, annual, and remedial training, as necessary, to address user behavior from detected security incidents;
- Creates Cybersecurity and Privacy Alerts and Notices that are emailed to workforce members;
- Provides Tips of the Day to workforce members;
- Conducts awareness events (phishing campaign, cybersecurity awareness month, etc.); and
- Displays posters.

c. The Agency must update literacy training and awareness content annually and/or following an update to policy, change in system, change in user roles, or as needed to address technology changes or patterns in threats and vulnerabilities in information systems.

d. The Agency must incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques. USAID

continuously improves security and privacy training based on feedback and administers training to address user behavior from detected security incidents.

e. The Agency must provide practical exercises that reproduce events and incidents. The Agency performs, at a minimum, bi-annual exercises using simulated phishing emails that mimic real-world scenarios. These exercises both imitate the adverse impacts of opening email attachments or clicking on embedded links as well as provide training and awareness through landing pages that include educational content to increase user knowledge and awareness of social engineering attacks.

f. The Agency must provide literacy training on recognizing and reporting potential indicators of insider threat.

1. SEC provides a required Insider Threat brief to all new USAID workforce members and all workforce members are required to complete it (see section **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 and how to report a related incident.

2. M/CIO, in collaboration with SEC, provides insider threat training as part of the annual cybersecurity training provided to all members of the workforce.

g. The Agency must provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining. The CISO provides literacy and awareness training:

1. As part of the initial security and privacy literacy training for new workforce members;

2. Annually as part of the cybersecurity and privacy refresher awareness training provided to all workforce members; and

3. Throughout the year via Tips of the Day and Notices to reinforce the message.

545.3.3.3 Role-Based Training (AT-3)

Effective Date: 12/28/2022

a. The Agency must provide role-based security and privacy training to individuals that are assigned significant security and/or PII processing responsibilities.

1. USAID provides role-based training that addresses general risk management and information security and privacy topics.

2. All workforce members with significant security and/or PII responsibilities (*e.g.,* SOs, ISSOs, system administrators, etc.) must:

- Complete role-based training specific to their security and PII processing responsibilities upon assignment to the role, and refresher training yearly thereafter.

- Complete additional role-based training as needed to address technology changes or patterns in threats and vulnerabilities in information systems.

Note: Privileged/elevated rights are suspended for personnel identified as having significant security and/or PII processing responsibilities who fail to comply with role-based training requirements.

3. SOs must identify personnel with significant security and/or PII processing 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.

b. The Agency must update role-based training content annually and/or following an update to policy, change in system, change in user roles, or as needed to address technology changes or patterns in threats and vulnerabilities in information systems.

c. The Agency must incorporate lessons learned from internal or external security or privacy incidents into role-based training.

545.3.3.4 Training Records (AT-4)
Effective Date: 12/28/2022

M/CIO must:

a. Document, monitor, track, and maintain annual security and privacy awareness and role-based training records.

b. Retain individual training records in accordance with USAID record retention policies (see **ADS 502mab, Strategic Objective Document Disposition Schedule**). Training records must include trainee name and position (if security or privacy role), as well as date and type of training received.

545.3.4 Audit and Accountability (AU)
Effective Date: 12/28/2022

The AU control family measures a system's audit capabilities, with the goal of ensuring that the system retains records of who has accessed the system and what they did while they were in it. AU controls assist the system and the Agency in detecting security violations, as well as performance and technical issues.

545.3.4.1 Policy and Procedures (AU-1)
Effective Date: xx/xx/xxx

The CISO must:

a. Develop, document, and disseminate to the AO, SOs, ISSOs, and other key information assurance personnel an Agency-level audit and accountability policy that:

1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

b. Designate a policy lead to manage the development, documentation, and dissemination of the audit and accountability policy.

c. Review and update the current audit and accountability policy annually and following changes to the status of the AIDNet, as needed.

SOs must:

i. Develop and document system-level procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls; and

ii. Review and update the current audit and accountability procedures annually and following any changes to the status of the AIDNet ATO or constituent systems under the SO's purview

545.3.4.2 Event Logging (AU-2)
Effective Date: 12/28/2022

The CISO must document both general and threat-specific logging and auditing guidance and SOs must document business specific logging guidance. The CISO and SOs must review the set of required auditable security events annually or more frequently upon changes to situational awareness of threats or vulnerabilities.

SOs must:

a. Ensure that information systems are capable of and configured to log CISO defined and business specific auditable security events;

b. Identify the types of events that the system is capable of logging in support of the

audit function;

c. Coordinate the event logging function with other organizational entities requiring audit- related information to guide and inform the selection criteria for events to be logged;

d. Specify the event types for logging within the system along with the frequency of (or situation requiring) logging for each identified event type;

e. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

f. Review and update the event types selected for logging quarterly.

545.3.4.3 Content of Audit Records (AU-3)

Effective Date: 12/28/2022

SOs must:

a. Ensure the information system has the capability to log auditable events that are sufficient in detail to facilitate the reconstruction of security-relevant events if compromise or malfunction occurs or is suspected.

b. Ensure that audit records contain information that establishes the following:

1. What type of event occurred;

2. When the event occurred;

3. Where the event occurred;

4. Source of the event;

5. Outcome of the event; and

6. Identity of any individuals, subjects, or objects/entities associated with the event.

c. If PII is included in the audit records involved (records such as time stamps, source and destination address, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked), analyze for and mitigate privacy risk(s).

d. Review audit records as specified in the SSP for that respective system. For more information.

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. A centralized auditing capability collects audit information from all system components into a system-wide (logical or physical) audit trail that correlates audit records across different repositories to gain Agency-wide situational awareness and provide a capability to centrally review and analyze audit records.

SOs must coordinate with the AO/CO to ensure that contracts and other agreements address the AU capability for systems not hosted on AIDNet operated on USAID's behalf.

545.3.4.4 Audit Log Storage Capacity (AU-4)

Effective Date: 12/28/2022

SOs must:

a. Ensure that sufficient audit log retention storage capacity is allocated to accommodate Agency-defined audit log retention requirements; and auditing is configured to reduce the likelihood of that capacity being exceeded. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

b. Conduct, in coordination with the system maintenance provider, an analysis and determination for increasing storage when storage capacity reaches 80 percent.

545.3.4.5 Response to Audit Logging Process Failures (AU-5)

Effective Date: 12/28/2022

SOs must:

a. Configure the Information System to alert in the event audit storage capacity is reached or exceeded, or in the event of audit processing failure;

b. Define in the SSP the designated personnel to be notified when audit storage capacity is reached or exceeded or when audit processing fails so that storage capacity can be increased to facilitate continuous audit event collection; and

c. Configure an alternate audit logging capability in the event of a failure in the primary audit logging process.

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

Effective Date: 12/28/2022

SOs must:

a. Ensure that audit records for Agency information systems are reviewed and analyzed at least weekly for potential impact of the inappropriate or unusual activity;

b. Adjust the audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information; and

c. Report unusual and suspicious activity or unexplained access attempts to the system or Mission ISSO and open a ticket with the M/CIO Service Desk at **cio-helpdesk@usaid.gov**.

M/CIO must:

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

ii. Provide and implement a capability to analyze and correlate audit records across different repositories to gain Agency-wide situational awareness.

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

Effective Date: 12/28/2022

SOs must:

a. Ensure that the information system provides and implements an audit record 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; and

b. Ensure that the information system provides the capability to process, sort, and search audit records for events of interest based on defined criteria.

545.3.4.8 Time Stamps (AU-8)

Effective Date: 12/28/2022

SOs must:

a. Ensure that information systems use internal system clocks to generate timestamps for audit records. Time service is critical to other security capabilities such as access control and identification and authentication.

b. Ensure that the time stamps generated by an Information System 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.

c. Ensure the information system synchronizes 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: 12/28/2022

SOs must:

a. Protect their audit records, logs, and any PII within the audit record from unauthorized change, access, or destruction;

b. Ensure that only explicitly authorized security professionals are given permissions and access to audit management functionality;

c. Implement an alert for personnel designated in the SSP upon detection of unauthorized access, modification, or deletion of audit information to reduce the risk of a vulnerability specific to the system, or the compromise of the audit records; and

d. Ensure that audit records are stored on a component running a different operating system than the subject system or component being audited.

545.3.4.10 Audit Record Retention (AU-11)

Effective Date: 12/28/2022

SOs must:

a. Retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes, including to provide support for after-the-fact investigations of incidents. Audit records must be retained for a minimum of 12 months in active data storage, and afterwards for a minimum of 18 months in cold data storage, and thereafter maintained for a minimum of 7 years in accordance with Agency record retention policies (refer to **ADS 502**).

b. Employ measures to ensure that long-term audit records generated by the system can be retrieved. Measures employed to help facilitate the retrieval of audit records include converting records to newer formats, retaining equipment capable of reading the records, and retaining the necessary documentation to help personnel understand how to interpret the records.

545.3.4.11 Audit Record Generation (AU-12)

Effective Date: 12/28/2022

SOs must ensure that information systems:

a. Provide an audit record generation capability for system components, auditable

events, and defined content;

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

c. Generate audit records for the specified event types.

545.3.5 Assessment, Authorization, and Monitoring (CA)
Effective Date: 12/28/2022

When an information system is acquired or developed, an SA&A, is required 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 Policy and Procedures (CA-1)
Effective Date: 12/28/2022

The CISO must:

a. Develop, document, and disseminate to the USAID workforce an Agency-wide assessment, authorization, and monitoring policy that:

1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Develop, document, and disseminate to SOs procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls.

c. Designate a policy lead to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures.

d. Review the policy and procedures at least annually and update them as needed or following system changes.

e. Maintain a repository for all Security Authorization Process documentation and modifications.

545.3.5.2 Control Assessments (CA-2)
Effective Date: 12/28/2022

SOs must:

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a security control assessment plan that describes the scope of the assessment, including:

1. Security and privacy controls and control enhancements in scope;

2. Assessment procedures to be used to determine control effectiveness; and

3. Assessment environment, team, and roles and responsibilities.

c. Acquire approval for the assessment plan from the AO or the designated representative prior to conducting the assessment.

The assessment must produce a Control Assessment Report that documents the results of the assessment and must provide the results of the security and privacy control assessment to M/CIO/IA, the CISO, CPO, and AO.

SOs must assess the security and privacy controls in their information systems and their environment of operation at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.

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. An independent assessor must assess systems and common control packages with a security categorization of high or moderate. A security and privacy 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 CISO must maintain a list of all the security and privacy control assessors, the systems that they assessed, and the dates when the assessments were completed.

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 SA&A process documented in the **IT Systems Accreditation RMF Handbook** (available on the **SA&A Process** page).

545.3.5.3 Information Exchange (CA-3) and Internal System Connections (CA-9)

Effective Date: 12/28/2022

M/CIO and SOs must authorize connections and exchange of information from USAID information systems to other information systems using 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 (IAAs), 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**.

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 and exchange of information of USAID information systems.

b. Document the interface characteristics, security requirements, controls, responsibilities for each system, 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.

d. Terminate the internal system connection and interconnection agreement upon determination that the connection is no longer needed for the transfer of information.

Note: Interconnections between systems require an ISA whenever there are two different AOs involved.

All interconnections and exchange of information 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: 12/28/2022

When information system or common control 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 remediation actions of the Agency to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and update the POA&Ms at least monthly, including updates to milestones, based on security monitoring activities.

SOs must ensure that information security and privacy requirements and POA&Ms are accurate, adequately funded, resourced, and documented in accordance with current OMB budgetary and regulatory guidance, Executive Orders, directives, and mandates. Detailed information for creating and managing POA&Ms appears in the **POA&M Management Guide for Documenting Weakness and POAM Process Guide** (available on the **SA&A Process** page)

545.3.5.5 Authorization (CA-6)

Effective Date: 12/28/2022

All USAID systems, including third-party systems and sites, must adhere to the standards defined in the SA&A process documented in the **IT Systems Accreditation RMF Handbook** (available on the **SA&A Process** page). 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, 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 can be accessed via a link to the security artifact templates on the **SA&A Process** page.

M/CIO will 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.

The AO must:

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

b. Assign SOs to all common control packages through a letter of designation. 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.

c. 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 or privacy of the system. A major change includes, but is not limited to:

1. Full version changes 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 or privacy posture of the network, system, or information.

d. Decommission operational systems if the SOs have not conducted continuous monitoring and do not have funding for a new SA&A. Prior to ATO expiration, M/CIO will notify the SO that the system will be decommissioned by a specific date and removed from the network if an ATO has not been issued by M/CIO.

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

f. Accept risks for all systems for which an ATO is granted.

In coordination with the CISO, the AO may grant a restricted authority to operate (RATO) for systems that are undergoing development testing or are in a prototype phase of development. However, such systems must not operate without an approved ATO or RATO.

Note: An RATO is legally binding written permission to conduct activities but under certain restrictions. RATOs must not be used for operational systems. The AO, in coordination with the CISO, may grant an RATO at their discretion. Systems under an RATO must not process sensitive information but may attach to system networks for testing.

SOs must:

- 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**;

- Employ **NIST SP 800-53, Rev. 5** (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 and privacy controls specific to the system and the security objective; and

- Ensure common control providers accept and authorize the use of those common controls inherited by their system(s).

545.3.5.6 Continuous Monitoring (CA-7)

Effective Date: 12/28/2022

M/CIO must:

a. Develop a continuous monitoring strategy (see the **Information Security 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 system-level security metrics to be monitored;

2. Methods and frequency by which the metrics will be monitored for assessment of control effectiveness, assessed, and reported;

3. Correlation and analysis of information generated by assessments and monitoring,

4. Response actions to address results of the analysis of control assessments and monitoring information, and

5. Reporting the security and privacy status of systems, on an ongoing basis, to the AO, CISO, CPO and other appropriate Agency officials, as necessary.

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 accordance with the ISCM Strategy.

d. Ensure risk monitoring is an integral part of the continuous monitoring strategy including effectiveness monitoring, compliance monitoring, and change monitoring.

SOs must perform and document continuous monitoring activities in accordance with the ISCM Strategy.

545.3.6 Configuration Management (CM)

Effective Date: 12/28/2022

Configuration management (CM) refers to the configuration of all hardware and software elements within information systems and networks. CM at 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 that documentation is updated in association with an approved change to a USAID system. The change management process must reflect 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 Policies and Procedures (CM-1)

Effective Date: 12/28/2022

The CISO must:

a. Develop, document, and disseminate to the USAID workforce an Agency-level configuration management policy that:

1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

b. Designate a policy lead to manage the development, documentation, and dissemination of the configuration management policy.

c. Review the policy annually and update it as required or following incidents that impact the system.

SOs must:

- Develop, document, disseminate, implement, and enforce system-level procedures in a System Security Plan (SSP) to comply with CM policy and associated controls;
- When considering proposed changes, ensure that CM processes for the system reflect the results of a security impact analysis (SIA) (refer to **NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems**, for more information); and
- Review and update the SSP annually and after a major change to the system.

545.3.6.2 Baseline Configuration (CM-2)

Effective Date: 12/28/2022

SOs must:

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

b. Review configuration baselines annually and update the baseline configuration as required, when system components are installed, upgraded, or when major changes to the system warrant;

c. Maintain currency, completeness, accuracy, and availability of the baseline configuration of the system using Agency Configuration Management Database (CMDB) automated tools, when possible;

d. Retain two previous versions of baseline configurations of the system to support rollback;

e. Coordinate with the CISO to establish specific configuration baselines for all network devices and endpoints, including mobile computing devices;

f. Ensure that configuration baselines are applied to all GFE computing devices prior to issuing them to workforce members; and

g. Ensure that processes for securing devices are documented and implemented and that the standard baseline configurations are reapplied to GFEs when they are returned prior to reissuing them.

Note: Due to its rapid response requirements, the Bureau for Humanitarian Assistance (BHA) 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 Security Assessment Report (SAR).

545.3.6.3 Configuration Change Control (CM-3)

Effective Date: 12/28/2022

M/CIO must:

a. Determine the types of changes to the system that are configuration-controlled, review, approve/disapprove with explicit consideration for security and privacy impact, document change decisions, implement approved changes, and retain change records for at least three years;

b. Monitor and review activities associated with configuration-controlled 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 and privacy representative must be a member of the change control board.

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

545.3.6.4 Impact Analyses (CM-4)

Effective Date: 12/28/2022

SOs must analyze proposed changes to their assigned systems to determine potential security and privacy impacts prior to change implementation and make recommendations based on that analysis.

After system changes, SOs must verify that the affected controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

545.3.6.5 Access Restrictions for Change (CM-5)

Effective Date: 12/28/2022

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

545.3.6.6 Configuration Settings (CM-6)

Effective Date: 12/28/2022

The CISO must establish and document baseline configuration settings for various IT equipment that reflect the most restrictive mode consistent with operational requirements (see the **M/CIO Security Baseline Guides** 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: 12/28/2022

SOs must:

a. Ensure that systems are configured to provide only USAID's mission essential

capabilities and that the relevant M/CIO-approved ports, protocols, software and/or services are documented in the SSP and reflected in the system baseline configurations to restrict the usage;

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

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

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

e. Identify software programs authorized to execute on the system by referencing the **Approved Products List (APL)**; and

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

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

545.3.6.8 System Component Inventory (CM-8)

Effective Date: 12/28/2022

SOs must:

a. Maintain an accurate list of all system components in the system, including but not limited to cloud, social media, and mobile devices;

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

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

d. Ensure the hardware inventory is at the level of granularity deemed necessary for tracking and reporting. The inventory specifications include:

1. Vendor/manufacturer name;

2. Hardware model number, item description, and serial number; and

3. Physical location of hardware.

e. Ensure the software inventory is at the granularity level deemed necessary for tracking and reporting, including:

1. Software name, version number, and description; and

2. Software license information including number of licenses, etc., as applicable.

SOs must ensure that the system component inventory is reviewed and updated as an integral part of the change management process and at a minimum annually.

M/CIO and/or SOs must on a continuous basis detect the presence of unauthorized hardware, software, and firmware components throughout the Agency and systems using USAID-approved automated mechanisms.

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

545.3.6.9 Configuration Management Plan (CM-9)

Effective Date: 12/28/2022

SOs must develop, document, and implement a CM Plan for their system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

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

c. Defines the configuration items for the system and place the configuration items under configuration management;

d. Obtain review and approval for configuration items from the system that will hosts the items; and

e. Protect the CM Plan from unauthorized disclosure and modification.

545.3.6.10 Software Usage Restrictions (CM-10)

Effective Date: 12/28/2022

SOs must:

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

b. Employ tracking systems for software usage 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 (see **Software and Hardware Approval Process**). Approval is based on an assessment of risk and the total life cycle cost (see **OMB Memorandum 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: 12/28/2022

Members of the workforce are not authorized to install software, in accordance with the **ADS 545mbd, Rules of Behavior for Users**. Members of the workforce 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.

545.3.6.12 Information Location (CM-12)

Effective Date: 12/28/2022

SOs must:

a. Identify and document the location of mission-critical data and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (*i.e.,* system or system components) where the information is processed and stored; and

d. Use automated tools to identify mission critical data on mass storage components (*e.g.,* storage area network [SANs]/shared drives, Google Drive/Team folders, S3 buckets, local, etc.) to ensure controls are in place to protect organizational information and individual privacy.

545.3.7 Contingency Planning (CP)
Effective Date: 12/28/2022

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 Policy and Procedures (CP-1)
Effective Date: 12/28/2022

The CISO must:

a. Develop, document, and disseminate to the USAID workforce an Agency-level contingency planning policy that:

1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Designate a policy lead to manage the development, documentation, and dissemination of the contingency planning policy.

c. Review the current contingency planning policy annually and update as needed.

SOs must:

- Develop, document, and disseminate to users system-level procedures to comply with contingency planning policies and associated contingency plan (CP) control requirements; and

- Review and update the current contingency planning procedures annually and following major system changes as needed.

545.3.7.2 Contingency Plan (CP-2)
Effective Date: 12/28/2022

SOs must:

- 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 system restoration without deterioration of the security safeguards originally planned and implemented;

7. Addresses the sharing of contingency information;

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

9. Identifies critical system assets supporting essential missions and business functions.

- 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.

- Review the CP annually.

- Update the CP to address changes to the Agency, system, or environment of operation and problems encountered during CP implementation, execution, or testing.

- Obtain approvals for the CP and subsequent updates from the AO and the BO(s) (if identified).

- Communicate CP changes to BO(s) and key contingency personnel.

- Distribute copies of the CP to the BO(s) and key contingency personnel, identified by name or by role in the plan.

- Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training.

- Protect the CP from unauthorized disclosure and modification.

545.3.7.3 Contingency Training (CP-3)

Effective Date: 12/28/2022

SOs must:

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

b. Review and update contingency training content annually, and following a major change to the system, or a change of SO.

545.3.7.4 Contingency Plan Testing (CP-4)

Effective Date: 12/28/2022

SOs must:

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

b. Test CPs for their 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: 12/28/2022

SOs must:

a. Establish an alternate storage site that:

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

2. Is geographically separated from the primary storage site sufficiently, 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 USAID 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. Explicit 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: 12/28/2022

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. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations, or put contracts in place to support delivery to the site within time periods consistent with RTO and RPO documented in the BIA for transfer/resumption;

c. Provide controls at the alternate processing site that are 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: 12/28/2022

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 sharing a single point 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 System Backup (CP-9)

Effective Date: 12/28/2022

SOs must:

a. Conduct or require backups of the following information:

- System, privacy-related and security-related documentation;
- User-level information; and
- System-level information.

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 ADS Chapter 545, 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 System Recovery and Reconstitution (CP-10)
Effective Date: 12/28/2022

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 Authentication (IA)
Effective Date: 12/28/2022

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.

Generally, identification is an assertion by the user of a unique identity (*e.g.,* a username); authentication is proof of that identity (*e.g.,* a password, PIV card, or token).

545.3.8.1 Policy and Procedures (IA-1)
Effective Date: 12/28/2022

The CISO must:

a. Develop, document, and disseminate to the USAID workforce an identification and authentication policy that:

1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Designate a policy lead to manage the development, documentation, and dissemination of the identification and authentication policy and procedures.

c. Review the current identification and authentication policy annually and update as needed.

SOs must:

- Develop, document, and disseminate to users system-level procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

- Review the current identification and authentication procedures annually and update, as needed; and

- Conduct annual reaccreditation of their systems mapped to **NIST 800-63-3, Digital**

Identity Guidelines, and assurance levels for Identity, Authentication, and Federation. Agencies are mandated in **OMB Memorandum M-19-17** to accredit their systems against the Digital Identity Risk Assessment (DIRA), which superseded M-04-04 eAuthentication Guidelines Mandate that was rescinded in May 2019.

545.3.8.2 Identification and Authentication (Organizational Users) (IA-2)

Effective Date: 12/28/2022

Organizational users include employees or individuals that organizations deem to have equivalent status of employees. At USAID, organizational users are defined as members of the workforce. 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 multi-factor authentication (MFA) for network access for all accounts, and MFA for local access for privileged accounts;

c. Implement replay-resistant authentication mechanisms for network access to privileged accounts. Replay-resistant techniques include approved **NIST 800-63-3** authenticators (for example: U2F and FIDO, FIDO2 and X509 protocols) that use stronger authentication, such as mobile push technology, out-of-band authentication that is more secure than one time passwords (OTP), and authentication that is not passed through the endpoint;

d. Implement Zero Trust Network Access (ZTNA) where MFA is not passed through, but rather occurs through a connection between the application and the backend system challenges, such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators;

e. Implement MFA using ZTNA principles. Trust no user of a device unless its identity can be verified by the issued government credential such as a USAID Non-Person Entity Certificate, following the USAID Certification Policy and Practice Statement; **NIST 800-157,Guidelines for Derived Personal Identity Verification (PIV) Credentials**, for mobile PIV-derived credentials; and USAID MFA standards;

f. Configure applications to consume derived credentials following **NIST 1800-12**, and **NIST 800-63-3**, and other approved authenticators; and

g. Ensure all MFA uses Agency-controlled certificates and hardware/software tokens issued directly to each authorized unique identity.

545.3.8.3 Device Identification and Authentication (IA-3)

Effective Date: 12/28/2022

SOs must ensure that the information system uniquely identifies and authenticates all

endpoints and mobile devices before establishing a local, remote, or network connection using bidirectional authentication that is cryptographically based.

M/CIO must ensure there are USAID Non-Person Entity device certificates on all USAID government furnished devices for appropriate identification and authentication. The device connection is based on risk-based scoring and adaptive authentication, *e.g.,* location, device type.

545.3.8.4 Identifier Management (IA-4)

Effective Date: Effective Date: 12/28/2022

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 ten years; and

e. Disabling the identifier after 90 days of inactivity.

545.3.8.5 Authenticator Management (IA-5)

Effective Date: 12/28/2022

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 based on risks to the system. SOs must ensure that the final restrictions and conditions are documented in the SSP.

SOs must manage information system authenticators by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- Establishing initial authenticator content for authenticators defined by the Agency;
- Ensuring that authenticators have sufficient strength for their intended use;
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- Changing default content of authenticators prior to information system installation;

- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- Changing/refreshing authenticators at a minimum of every 90 days;
- Protecting authenticator content from unauthorized disclosure and modification;
- Requiring individuals to take specific security safeguards to protect authenticators and implementing mechanisms to facilitate such safeguards; and
- Changing authenticators for group/role accounts when membership to those accounts changes.

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

- Enforces minimum password complexity of at least 12 characters, with a mix of at least one character from each of three of the following four-character types: uppercase letters, lowercase letters, numbers, and special characters (refer to **ADS 545mau, Password Creation Standards** for more information);
- Enforces changes to at least four changed characters when new passwords are created;
- Stores and transmits only encrypted passwords;
- Enforces password minimum and maximum lifetime restrictions, with no minimum lifetime and a maximum lifetime of 90 days;
- Prohibits password reuse for 24 generations;
- Allows the use of a temporary password for system logons only with an immediate change upon first-time logon to a new password; and
- Prevents embedding passwords in scripts or source code.

SOs must ensure the information system does the following for PKI-based authentication (see section **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, 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, as follows:

a. The CISO must approve all biometric authentication methods;

b. When biometric authentication methods are in use, authentication procedures must be developed and implemented;

c. Members of the workforce must receive training in the secure use of biometric devices; and

d. Biometrics that are captured or transmitted by the Agency must be protected with the use of approved encryption mechanisms:

1. When biometrics are used for authentication, a PIN or passcode must also be used for MFA.

2. All PINs and passcodes must be a minimum of six characters.

USAID workforce members 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 to 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.

For other approved **NIST SP 800-63** authenticators, remote identity proofing may take place for Identity and Authentication Assurance level 2 (IAL/ALL2).

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 systems requiring encryption must follow these standards:

a. Must use: FIPS 197, Advanced Encryption Standard (AES), algorithms with at least 256-bit encryption validated under **FIPS 140-3**, National Security Agency (NSA) Type 2, or Type 1 encryption.

b. Must *not* use:

- Triple Data Encryption Standard (3DES)
- FIPS 140-1

SOs must:

- Develop and maintain encryption plans for sensitive information systems requiring encryption, and
- Use only cryptographic modules that are **FIPS 197** AES-256 compliant and have received **FIPS 140-3** validation at the level appropriate to their use.

545.3.8.6 Authentication Feedback (IA-6)

Effective Date: Effective Date: 12/28/2022

SOs must configure the IS 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: 12/28/2022

SOs must implement mechanisms in the IS 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 140-3** 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: 12/28/2022

Non-organizational users are IS users other than the organizational users covered by IA-2 (in section **545.3.8.2, Identification and Authentication (Organizational Users) (IA-2)**).

SOs must:

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

b. Ensure that the information system:

1. Incorporates multiple factors in one of two ways: (a) Multiple factors are

presented to the verifier; or (b) Some factors are used to protect a secret that will be presented to the verifier;

2. Accepts only external authenticators that are NIST-compliant; and document and maintain a list of accepted external authenticators; and

3. Employs only FICAM-approved information system components in enterprise level information systems to accept on NIST approved third-party credentials

Identity verification or authentication, known as e-authentication, secures online government services. 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 (FICAM) Trust Framework Provider Adoption Process (TFPAP) can make the determination. For more information on the FICAM initiative, see **Idmanagement.gov**.

545.3.8.9 Digital Signature Using Personal Identity Verification (PIV) Card

Effective Date: 12/28/2022

The term *digital signature* means a method of signing an electronic message and/or document that (a) identifies and authenticates a particular person as the source of the electronic message; and (b) indicates the person's approval of the information contained in the electronic message. The Agency, in compliance with **OMB Circular No. A-130**, **NIST SP 800-63**, and **HSPD-12**, has identified the use of a Personal Identity Verification (PIV) or PIV Alternative (PIV-A) card (referred to as PIV throughout this section) as a sufficiently strong authentication mechanism for use on official documents.

A PIV electronically-generated signature is acceptable and legally binding when signing a document in digital format. A PIV card mitigates security vulnerabilities by providing authentication, ensuring the identity of the signer.

545.3.8.10 Re-Authentication (IA-11)

Effective Date: 12/28/2022

SOs must configure their systems to:

a. Require users to re-authenticate periodically, *e.g.,* when there are changes to users roles and/or to the system's security status; the execution of privilege functions occurs; devices are locked; after a fixed time and/or users are logged out of the system.

b. Periodically re-authenticate subscriber sessions as described in **NIST 800-63B**, Section 7.2:

1. At Authentication Assurance Level 1 (AAL1), re-authentication of the subscriber must be repeated at least once every 30 days during an extended usage session, regardless of user activity. The session must be terminated

(*i.e.,* logged out) when this time limit is reached.

2. Periodic re-authentication of sessions must be performed to confirm the continued presence of the subscriber at an authenticated session (*i.e.,* that the subscriber has not walked away without logging out).

c. For screen lock outs, require re-authentication via PIV of MFA authenticator; and

d. Meet AAL and IAL accreditation requirements, outlined in the **USAID Digital Identity Risk Assessment (DIRA) Guidelines**. As the assurance level is identified, the re-authentication for that level must be assigned.

545.3.8.11 Identity Proofing (IA-12)

Effective Date: 12/28/2022

SOs must configure their systems to:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines, such as **NIST 800-63A, Enrollment and Identity Proofing**;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

SOs must:

1. Require evidence of individual identification be presented to the registration authority;

2. Require that the presented identity evidence be validated and verified through Digital Identity Guidelines per **OMB Memorandum M-20-04** and the Agency Office of the General Counsel's **Certification Regarding the Validity of Documents Provided During USAID Virtual Identity Proofing**;

3. Require that a notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record; and

4. Accredit system assurance levels using the updated ICAM Digital Identity Risk Assessment (DIRA) as part of the SA&A process.

545.3.9 Incident Response (IR)

Effective Date: 12/28/2022

Incident Management and Response is an important component of 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 Policy and Procedures (IR-1)

Effective Date: 12/28/2022

The CISO must:

a. Develop, document, and disseminate to USAID workforce an incident response policy that:

1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

b. Designate a policy lead to manage the development, documentation, and dissemination of the incident response policy.

c. Review the current incident response policy annually and update as needed.

SOs must:

1. Coordinate with the CISO to develop, document, and disseminate to users incident response procedures to facilitate the incident response policy and associated incident response controls.

2. Review the current incident response procedures annually and update the procedures as needed; and review following system boundary, SO, and ISSO changes, and based on lessons learned from cyber or privacy incidents.

545.3.9.2 Incident Response Training (IR-2)

Effective Date: 12/28/2022

As part of the continuous incident response capability, the CISO and SOs must ensure that members of the workforce with incident response roles and responsibilities are trained on how to identify and respond to a breach, including USAID’s process for reporting a breach, within 30 calendar days of assignment and provide refresher training annually, as well as review and update incident response training content annually and following system boundary changes.

545.3.9.3 Incident Response Testing (IR-3)

Effective Date: 12/28/2022

In coordination with CISO, SOs must test annually the incident response capability with

tabletop exercises and use documented results to validate and/or improve the incident response effectiveness with the necessary parties involved with incident responding.

545.3.9.4 Incident Handling (IR-4) / Incident Monitoring (IR-5)

Effective Date: 12/28/2022

The CISO must implement an incident handling procedure to include an Agency ticketing system to assist in tracking of security/privacy incidents and in collection and analysis of incident information.

The ticketing system 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 the workforce to report suspected security incidents to the organizational incident response capability as soon as discovered and report security incident information to designated authorities;

3. SOs and ISSOs must document information system-specific service desk and incident handling procedures in their information system's SSP and Incident Response Plan (IRP); and

4. Support the incident handling process using system level automated log retention capability that supports the collection of required logs and forensic analysis.

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the Agency.

545.3.9.5 Incident Reporting (IR-6) / Incident Response Assistance (IR-7)

Effective Date: 12/28/2022

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.

A system user must report any potential or confirmed security incidents as soon as discovered or within one hour to the M/CIO Service Desk at **cio-helpdesk@usaid.gov**.

All members of the workforce must immediately report all potential and actual privacy breaches or incidents to both the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** and the Privacy Program at **privacy@usaid.gov**, regardless of the format of the PII (*i.e.,* oral, paper, or electronic) or the way the incidents might have occurred (see ADS 508, Privacy Program for information on Privacy Incident Reporting).

System Owners must identify service providers' incident response team members and establish a direct, cooperative relationship between the vendor incident response capability and theirs to ensure proper lines of communication regarding incident information to the provider of the product or service and other organizations involved in the supply chain.

If a user knows or suspects that their government issued GFE, including Mobile Device (MD), has been compromised, they must immediately turn off their GFE and notify the M/CIO Service Desk at **cio-helpdesk@usaid.gov**. The user will be provided further guidance from the Service Desk or an ISSO. The user must not allow the compromised/possibly compromised GFE to connect to any networks (wireless or wired).

545.3.9.6 Incident Response Plan (IR-8)

Effective Date: 12/28/2022

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, review and approve the roadmap annually, and update it as needed;

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;

h. Address the sharing of incident information; and

i. Approve the incident response roadmap/plan.

SOs must:

1. Develop an IRP for implementing the incident response capability for their systems, review the plan annually, and update the plan as needed;

2. Distribute copies of the IRP to all personnel on the IRP's distribution list;

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

4. Communicate incident response plan changes to all personnel on the IRP's distribution list; and

5. Protect the plan from unauthorized disclosure and modification.

545.3.9.7 Information Spillage Response (IR-9)

Effective Date: 12/28/2022

The CISO must develop an information spillage response capability to identify and sanitize computers and mobile devices affected by a security or privacy incident. NIST defines information spillage as an instance in which sensitive information (*e.g.,* classified information, SBU, or PII) is inadvertently placed on an information system that is not authorized to process this type of information.

The program must contain the guidance to perform the following actions:

a. Identify the specific information involved in the system contamination.

b. Alert the appropriate parties of the information spill using a method of communication not associated with the spill:

- Alert USAID SEC and USAID Computer Incident Response Team (CSIRT) if the spillage information contains classified information, per **ADS 552**; and

- Alert the M/CIO Service Desk and Privacy team immediately on all potential and actual privacy breaches or incidents by calling (202) 712-1234 or emailing **cio-helpdesk@usaid.gov** and **privacy@usaid.gov**, respectively, regardless of the format of the PII (oral, paper, or electronic) or the way the incidents might have occurred, per **ADS 508**.

c. Validate spillage material is properly identified and requires remediation.

d. Isolate the contaminated system or system component.

e. Identify other systems or system components that may have been subsequently contaminated.

f. Eradicate the information from the contaminated system or component through validated standards.

g. Perform the following additional actions:

- Report the spillage to appropriate parties; and
- Restore affected systems back to service.

545.3.10 Maintenance (MA)

Effective Date: 12/28/2022

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 Policy and Procedures (MA-1)

Effective Date: 12/28/2022

The CISO must:

a. Develop, document, and disseminate to the USAID workforce personnel or roles an Agency level systems maintenance policy that:

1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among Agency Operational Units, and compliance; and

2. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Designate a policy lead to manage the development, documentation, and dissemination of the maintenance policy; and

c. Review the current maintenance policy annually and update the policy as needed.

SOs must:

1. Develop, document in the SSP, and disseminate to users procedures to facilitate the implementation of the maintenance policy and associated maintenance security controls; and

2. Review the procedures and applicable controls annually and update as needed and following major system changes.

545.3.10.2 Controlled Maintenance (MA-2)
Effective Date: 12/28/2022

SOs must:

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

b. Approve and monitor all maintenance activities, whether performed on site or remotely, and whether the system or system components are 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, repairs, or replacement.

d. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement.

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

f. Disable maintenance ports during normal operations.

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: 12/28/2022

SOs must:

a. Approve, control, and monitor the use of information system maintenance tools via the M/CIO managed Software/Hardware Request (SHR) or Architecture Review

Board (ARB).

b. Review previously approved system maintenance tools annually.

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

1. **Inspect Tools**: Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications;

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

3. **Prevent Unauthorized Removal**: Prevent the removal of maintenance equipment containing organizational information by verifying that there is no organizational information contained on the equipment, sanitizing or destroying the equipment, retaining the equipment within the facility; or obtaining an exemption from M/CIO/IA explicitly authorizing removal of the equipment from the facility.

545.3.10.4 Non-Local Maintenance (MA-4)

Effective Date: 12/28/2022

SOs must:

a. Approve and monitor non-local maintenance and diagnostic activities;

b. Allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ replay resistant authentication in the establishment of non-local maintenance and diagnostic sessions;

d. Maintain records for non-local maintenance and diagnostic activities; and

e. Terminate session and network connections when non-local maintenance is completed.

1. Log AU-2 defined audit events for nonlocal maintenance and diagnostic sessions; and

2. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

545.3.10.5 Maintenance Personnel (MA-5)

Effective Date: 12/28/2022

SOs must:

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

b. Verify that non-escorted personnel performing maintenance on the system possess the 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: 12/28/2022

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)
Effective Date: 12/28/2022

The MP control family addresses Agency and system protections over digital and non-digital media. Protections include restricting physical and digital access and ensuring accountability, labeling sensitive information, and ensuring information removed from media cannot be retrieved or reconstructed.

545.3.11.1 Policy and Procedures (MP-1)
Effective Date: 12/28/2022

The CISO must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency media protection policy that:

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Review the media protection policy annually and update, as needed;

c. Designate a policy lead to manage the development, documentation, and dissemination of the media protection policy.

SOs must:

1. Develop, document, implement, and disseminate to users system-level procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

2. Review media protection procedures at least annually and update as needed, and after major system changes. 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: 12/28/2022

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

Members of the workforce and others working on behalf of USAID must not:

- Use non-government approved/procured removable media (USB drives, in particular);

- Connect non-government media to USAID equipment or networks; and

- Use non-government approved media to store USAID sensitive information.

545.3.11.3 Media Marking (MP-3)
Effective Date: 12/28/2022

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 if 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: 12/28/2022

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 persons; and

b. Protect the following system media types until the media is destroyed or sanitized using Agency approved equipment, techniques, and procedures:

- Hardcopy Material – Printed material, including reports, emails, briefings, manuals, guidance, letters, and memoranda

- Electronic Storage Media – Includes but is not limited to magnetic storage media such as hard disk drives; optical storage media such as CDs and DVDs; solid-state storage media, including USB drives; and hardcopy materials, including reports, emails, briefings, manuals, guidance, letters, and memoranda.

545.3.11.5 Media Transport (MP-5)

Effective Date: 12/28/2022

All members of the workforce must:

a. Protect and 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** for the transportation or mailing of sensitive media. SOs must reference these guidelines or establish procedures aligned to these guidelines in the system SSP.

d. Employ an identified custodian during transport of system media outside of controlled areas.

545.3.11.6 Media Sanitization (MP-6)

Effective Date: 12/28/2022

The Agency has established Electronic Media Sanitization Standards that must be followed by all system stakeholders.

SOs must:

a. 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.

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information outlined in **NIST SP 800-88**.

c. Provide the capability to purge or wipe information from mobile devices when the device is reported as lost.

d. Test sanitizing equipment and procedures periodically to verify that the equipment functions properly and that the procedures are effective.

e. Maintain records of the sanitization and disposition of the information system's storage media.

f. Use cryptographic erase for sanitization. Cryptographic erase is a method of sanitization where the media encryption key is sanitized making recovery infeasible for cloud systems.

g. Enforce dual authorization for the sanitization of IS storage media to help ensure that system media sanitization cannot occur unless two technically qualified individuals conduct the designated task.

h. Provide the capability to purge or wipe information from organizational systems and system components if systems or components are obtained by unauthorized individuals.

545.3.11.7 Media Use (MP-7)

Effective Date: 12/28/2022

The CISO restricts the use of portable storage media, such as non-approved USB storage drives, flash drives, and non-approved mobile devices on all USAID information systems. Automated capabilities must be used to detect the presence of unauthorized devices on all USAID networks/information systems.

The CISO prohibits the use of sanitization-resistant media in all Agency systems.

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

545.3.11.8 Media Downgrading (MP-8)

Effective Date: 12/28/2022

The CISO must establish a system media downgrading process that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information.

SOs must:

a. Identify USAID system media requiring downgrading and verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations

of the potential recipients of the downgraded information per the established process;

b. Ensure that system media containing classified information has been properly downgraded prior to release to individuals without required access authorizations;

c. Document the system media downgrading actions; and

d. Test downgrading equipment and procedures annually to ensure that downgrading actions are being achieved.

545.3.12 Physical and Environmental Protection (PE)

Effective Date: 12/28/2022

The PE control family addresses Agency and system measures to protect systems, the buildings that house them, and related supporting infrastructures against physical threats. The controls cover buildings that house system and network components, the supporting facilities that are required to maintain operations, and natural and manmade threats and disasters that may affect the facilities and their operations.

545.3.12.1 Policy and Procedures (PE-1)

Effective Date: 12/28/2022

The Agency must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency physical and environmental protection policy that:

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Review the physical and environmental protection policy annually and update, as needed.

c. Designate a policy lead to manage the development, documentation, and dissemination of the physical and environmental protection policy.

SOs must:

1. Develop, document, implement, and disseminate to users system-level procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

2. Review physical and environmental protection procedures at least annually and update, as needed.

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, Domestic Security Programs**, **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: 12/28/2022

The Agency must:

a. Develop and maintain a current a list of approved individuals with authorized access to the facility where a system resides (except for those areas within the facility officially designated as publicly accessible);

b. Review and approve the access list detailing authorized facility access by individuals daily;

c. Issue authorization credentials for facility access; and

d. Remove individuals from the access list when access to the facility is no longer required.

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: 12/28/2022

The Agency must:

a. Enforce physical access authorizations by controlling ingress/egress at entry/exit points to the facility where a system resides by verifying individual access authorizations before granting access with physical access controls or guards;

b. Maintain physical access audit logs and access records for facility entry/exit points;

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 its control;

g. Annually inventory physical access devices; and

h. Change combinations and replace keys when compromised or lost, and when individuals, possessing the keys or combinations, are transferred or terminated.

545.3.12.4 Access Control for Output Devices (PE-5)

Effective Date: 12/28/2022

The Agency must control physical access to standard approved output devices (such as monitors, printers, headphones, computer speakers, projectors, global positioning systems [GPS], sound cards, video cards, braille readers, and speech-generating devices) to prevent unauthorized individuals from obtaining the information converted to a human readable form. Output devices must be secured in locked rooms or other controlled areas with access restricted to only authorized individuals and monitored by organizational personnel.

545.3.12.5 Monitoring Physical Access (PE-6)

Effective Date: 12/28/2022

The Agency must:

a. Monitor physical access to facilities where 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 access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

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

Effective Date: 12/28/2022

The Agency must:

a. Ensure the protection of 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: 12/28/2022

SOs must:

a. Coordinate with Agency designees or contractors to ensure an emergency shutoff capability for a system and/or its 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 an uninterruptible power supply exists for the system to facilitate an orderly shutdown of the 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 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: 12/28/2022

SOs must:

a. Ensure that automated fire suppression and detection systems, supported by an independent energy source, are employed and maintained; and

b. Ensure that the fire detection systems that activate automatically and notify personnel and the Bureau for Management, Office of Management Services (M/MS) and emergency responders in the event of a fire.

545.3.12.9 Environmental Controls (PE-14)
Effective Date: 12/28/2022

SOs must coordinate with Agency designees or contractors to ensure that temperature, pressure, radiation, and humidity levels within the facility where the 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: 12/28/2022

SOs must coordinate with Agency designees or contractors to ensure that the 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: 12/28/2022

SOs must coordinate with Agency designees or contractors to ensure that 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: 12/28/2022

The Agency must:

a. Determine and document the alternate work sites allowed for use by employees;

b. 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

c. Provide a means for employees to communicate with information security personnel and privacy personnel in case of security or privacy incidents or other problems.

545.3.13 Planning (PL)
Effective Date: 12/28/2022

The PL control family covers the Agency's information security planning for the systems that support it to ensure that security is sufficient to counter the risk associated with operating the systems.

545.3.13.1 Policy and Procedures (PL-1)
Effective Date: 12/28/2022

The Agency must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency privacy and security planning policy that:

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, Executive Orders, directives, regulations,

policies, standards, and guidelines.

b. Review the planning policy annually and update, as needed.

c. Designate a policy lead to manage the development, documentation, and dissemination of the planning policy.

The Agency must:

1. Develop, document, implement, and disseminate to users a system-level privacy and security planning procedures to facilitate the implementation of the planning policy and the associated planning controls; and

2. Review privacy and security planning procedures at least annually, and update as needed, and following major changes.

545.3.13.2 System Security and Privacy Plans (PL-2)

Effective Date: 12/28/2022

USAID must develop general organizational security and privacy plans, which encompass the Agency's vision. The CISO and SAOP are responsible for ensuring the Agency plans are established and reviewed annually and updated as necessary.

SOs must ensure that each Agency system has its own security and privacy plans, which are reviewed annually and updated as necessary.

SOs must:

a. Develop security and privacy plans for the system that:

1. Are consistent with the organization's enterprise architecture;

2. Explicitly define the constituent system components;

3. Describe the operation context of the system in terms or mission and business processes;

4. Identify the individuals who fulfill system roles and responsibilities;

5. Identify the information types that are processed, stored, and transmitted by the system;

6. Provide the security categorization of the system, including supporting rationale;

7. Describe the specific threats to the system that are of concern to the organization;

8. Provide the results of a privacy risk assessment for systems processing PII;

9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

10. Provide an overview of the security and privacy requirements for the system;

11. Identify any relevant control baselines or overlays, if applicable;

12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for tailoring decisions;

13. Include risk determinations for security and privacy architecture and design decisions;

14. Include security and privacy related activities affecting the system that require planning and coordination with the CISO and CPO, or their designees;

15. Are reviewed and approved by the AO or designated representative for a security plan and the SAOP or designated representative for a privacy plan prior to plan implementation.

b. Distribute copies of the security and privacy plans and communicate subsequent changes to the plans to AO, SAOP, CPO, CISO, ISSO, and other designated authorized officials, as needed.

c. Update the privacy and security plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments.

d. Protect the security and privacy plans from unauthorized disclosure and modification.

e. 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.

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

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

Effective Date: 12/28/2022

Agency ROB in **ADS 545mbd** must be acknowledged and documented prior to

individuals receiving physical and/or logical access to USAID facilities and information systems and affirmed on an annual basis thereafter to maintain access. The ROB must describe the responsibilities and expected behavior of users who have access to USAID facilities, data, and systems, including privacy and security duties.

The Agency rules must include restrictions on:

a. Using social media, social networking sites, and external sites/applications on GFE;

b. Posting organizational information on public websites;

c. Use of organization-provided identifiers (*e.g.,* email addresses) and authentication secrets *(e.g.,* passwords) for creating accounts on external sites/applications;

d. Use of mobile devices; and

e. Handling of PII and sensitive information.

System-specific access may require that SOs obtain a signed system-specific ROB document from users before access is granted to them. A revised ROB may be used if it addresses any issues specific to that system. SOs must review and update the system-specific ROB document and obtain a new signature from each user documenting their acceptance.

The CISO and CPO must develop, review, and update **ADS 545mbd** annually or as required. SOs must develop, review, and update their system-specific ROB annually or as required.

A signed ROB document must be retained and available.

For more information, see **ADS 545mbd**.

545.3.13.4 Security and Privacy Architectures (PL-8)

Effective Date: 12/28/2022

The CISO and CPO must:

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

b. Ensure that systems comply with the USAID enterprise architecture (EA) and security architecture; or

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

SOs must:

1. Develop security and privacy architectures for their systems that:

- Describe the requirements and approach for protecting the confidentiality, integrity, and availability of organizational information;
- Describe the requirements and approach for processing PII to minimize privacy risk to individuals;
- Describe how the architectures are integrated into and support the enterprise architecture; and
- Describe any assumptions about, and dependencies on, external systems and services.

2. Review and update the security and privacy architectures at least annually to reflect changes in the enterprise architecture.

3. Reflect planned architecture changes, concept of operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

545.3.13.5 Central Management (PL-9)
Effective Date: 12/28/2022

The CISO must centrally manage all controls and related processes that are suitable for central management based on resources and capabilities.

545.3.13.6 Baseline Selection (PL-10)
Effective Date: 12/28/2022

SOs must select a control baseline for their systems.

545.3.13.7 Baseline Tailoring (PL-11)
Effective Date: 12/28/2022

ISSOs must tailor the selected control baseline for the system they are supporting by applying specified tailoring actions.

545.3.14 Personnel Security (PS)
Effective Date: 12/28/2022

The PS control family seeks to minimize the risk that workforce members pose to organizational assets through the malicious use or exploitation of their legitimate access to the organization’s resources. Because employees may have access to extremely sensitive, confidential, or proprietary information, the disclosure of which can destroy an organization’s reputation or cripple it financially, organizations must be vigilant when recruiting and hiring new employees, as well as when an employee transfers or is terminated.

545.3.14.1 Policy and Procedures (PS-1)

Effective Date: 12/28/2022

The Agency must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency personnel security policy that:

- Addresses Position Risk Designation (PS-2), Personnel Screening (PS-3), Personnel Termination (PS-4), Personnel Transfer (PS-5), Access Agreements (PS-6), External Personnel Security (PS-7), Personnel Sanctions (PS-8), and Position Descriptions (PS-9);

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

b. Review the personnel security policy annually and update as needed.

c. Designate a policy lead to manage the development, documentation, and dissemination of the personnel security policy.

The Agency must:

1. Develop, document, implement, and disseminate to the USAID workforce personnel security procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls; and

2. Review personnel security procedures at least annually and update as needed and following major changes.

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

545.3.14.2 Position Risk Designation (PS-2)

Effective Date: 12/28/2022

The Agency must assign a risk designation to all organizational positions; establish screening criteria for individuals filling those positions; and review and update position risk designations, as necessary.

545.3.14.3 Personnel Screening (PS-3)
Effective Date: 12/28/2022

The Agency must screen individuals prior to authorizing access to its systems and must rescreen individuals in accordance with the Agency's background investigation policy.

545.3.14.4 Personnel Termination (PS-4)
Effective Date: 12/28/2022

Upon termination of an individual's employment, the Agency must:

a. Disable system access within 24 hours;

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of the importance of safeguarding sensitive information;

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by the terminated individual.

545.3.14.5 Personnel Transfer (PS-5)
Effective Date: 12/28/2022

When workforce members are reassigned or transferred to other positions within the USAID, the Agency must:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities;

b. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

c. Notify appropriate personnel within a reasonable period of time.

545.3.14.6 Access Agreements (PS-6)
Effective Date: 12/28/2022

The SOs must:

a. Develop and document access agreements for systems;

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

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

- Sign appropriate access agreements prior to being granted access; and
- 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, ROB, and conflict-of-interest agreements.

545.3.14.7 External Personnel Security (PS-7)

Effective Date: 12/28/2022

Third-party providers include, for example, contractors and other organizations providing system development, IT services, outsourced applications, and network and security management.

ISSOs must ensure that SOs, CORs, or other designees:

a. Establish workforce 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 within one business day of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges or who have information system privileges; and

e. Monitor provider compliance.

Accordingly, contracts with third party providers must include the appropriate clauses and contract requirements referenced in **ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology**.

545.3.14.8 Personnel Sanctions (PS-8)

Effective Date: 12/28/2022

The Agency must:

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures, whether or

not the failure results in criminal prosecution;

b. Notify supervisors and/or HCTM within the same business day when a formal employee sanctions process is initiated by identifying the individual sanctioned and the reason for the sanction; and

c. Consider the appropriate remediation, including termination of access to USAID information systems and facilities for USAID contractors and external users who fail to comply with Agency security policies, whether or not the failure results in criminal prosecution; and

Any person who improperly discloses sensitive and/or non-public information may be subject to administrative, criminal, or civil penalties and sanctions, consistent with applicable laws, regulations, policies (e.g., the Trade Secrets Act (18 U.S. Code § 1905), Standards of Ethical Conduct for Federal Employees (5 cfr part 2635), **ADS 109** and **ADS 487saa**).

For more information regarding disciplinable offenses, see **ADS Chapter 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct – Civil CFRService** or **ADS Chapter 485, Disciplinary Action - Foreign Service**, and **5 CFR, section 2635.704, "Use of Government Property**."

545.3.14.9 Position Descriptions (PS-9)

Effective Date: 12/28/2022

The Office of Human Capital and Talent Management (HCTM) incorporates security and privacy roles and responsibilities into organizational position descriptions.

545.3.15 Personally Identifiable Information Processing and Transparency (PT)

Effective Date: 12/28/2022

The PT control family addresses the Agency's collection and processing of PII, establishing Agency and system authorization and notification processes to limit collection to only what is needed and to protect that which is collected.

545.3.15.1 Policy and Procedures (PT-1)

Effective Date: 12/28/2022

The USAID Privacy Program must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency-wide PII processing and transparency policy that:

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

b. Review the PII processing and transparency policy annually and update as needed and following any new Executive Orders, OMB memoranda, NIST guidance, or Agency Directives that affect privacy policy and procedures or lessons learned from a process shortfall.

c. Designate a CPO to manage the development, documentation, and dissemination of the PII processing and transparency policy.

545.3.15.2 Authority to Process Personally Identifiable Information (PT-2)
Effective Date: 12/28/2022

The USAID Privacy Program will:

a. Determine and document policies in **ADS 508**, which permit the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal (collectively referred to as “processing”) of PII; and

b. Restrict the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal (collectively referred to as “processing”) of PII to only that which is authorized.

545.3.15.3 Personally Identifiable Information Processing Purposes (PT-3)
Effective Date: 12/28/2022

The USAID Privacy Program will:

a. Identify and document the purpose(s) for processing PII;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the processing of PII to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing PII and implement privacy continuous monitoring to ensure that any changes are made in accordance with any Privacy Act Statements, authorities to collect, and System of Record Notices (SORNs) published in the Federal Register.

545.3.15.4 Consent (PT-4)
Effective Date: 12/28/2022

USAID will implement opt-in options for information collections, as appropriate, for individuals to consent to the processing of their PII prior to its collection. This implementation facilitates' informed decision-making to:

a. Allow individuals to tailor processing permissions to selected elements of PII; and

b. Implement procedures for individuals to revoke consent to the processing of their personally identifiable information.

545.3.15.5 Privacy Notice (PT-5)

Effective Date: 12/28/2022

USAID will provide notice to individuals about the processing of PII that:

a. Is available to individuals upon first interacting with an organization, and subsequently when PII is collected;

b. Is clear and easy-to-understand, expressing information about PII processing in plain language;

c. Identifies the authority that authorizes the processing of PII;

d. Identifies the purposes for which personally PII is to be processed;

e. Includes the circumstances under which PII may be disclosed and consequences, if any, of not providing requested information;

f. Presents notice of PII processing to individuals at a time and location where the individual provides PII or in conjunction with a data action;

g. Includes Privacy Notices for non-Privacy Act information collections that involve PII; and

h. Includes Privacy Act statements for information collections that will be maintained in a Privacy Act system of records or provides Privacy Act statements on separate forms that can be retained by individuals.

545.3.15.6 System of Records Notice (PT-6)

Effective Date: 12/28/2022

For information that will be maintained in a Privacy Act system of records, the USAID Privacy Program will:

a. Draft systems of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to OMB and appropriate congressional committees for advance review;

b. Publish system of records notices (SORNs) in the Federal Register;

c. Keep the SORNs accurate, up-to-date, and scoped in accordance with policy;

d. Review all routine uses published in the SORN annually to ensure continued accuracy and to ensure that routine uses continue to be compatible with the purpose for which the information was collected; and

e. Review all Privacy Act exemptions claimed for the system of records annually to ensure they remain appropriate and necessary in accordance with law, have been promulgated as regulations, and are accurately described in the system of records notice.

545.3.15.7 Specific Categories of Personally Identifiable Information (PT-7)

Effective Date: 12/28/2022

USAID will apply need to know based on business functions and user roles for PII.

When a system processes Social Security numbers (SSNs), USAID must:

a. Eliminate unnecessary collection, maintenance, and use of SSNs, and explore alternatives to their use as a personal identifier;

b. Ensure that it does not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN; and

c. Inform any individual who is asked to disclose their SSN whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

USAID prohibits the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

545.3.15.8 Computer Matching Requirements (PT-8)

Effective Date: 12/28/2022

When a system or organization processes information for the purpose of conducting a matching program, USAID must:

- Obtain approval from the Data Integrity Board to conduct the matching program;
- Develop and enter into a computer matching agreement;
- Publish a matching notice in the Federal Register;

- Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and

- Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

545.3.16 Risk Assessment (RA)
Effective Date: 12/28/2022

The RA control family covers how the Agency performs risk assessments on information systems to identify and prioritize the risks the system poses to USAID operations, assets, the workforce, and the Nation based on system threats, and vulnerabilities and the likelihood they will occur or be exploited.

545.3.16.1 Policy and Procedure (RA-1)
Effective Date: 12/28/2022

The CISO must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency risk assessment policy that:

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Review the risk assessment policy annually and update as needed.

c. Designate a policy lead to manage the development, documentation, and dissemination of the risk assessment policy.

SOs must:

1. Develop, document, implement, and disseminate to the USAID workforce risk assessment procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; and

2. Review risk assessment procedures at least annually and update as needed and following major system changes.

545.3.16.2 Security Categorization (RA-2)
Effective Date: 12/28/2022

FIPS 199 establishes security categories for systems based on the potential impact to

the organization if certain events occur that affect the system. 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; and

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, including loss of life or serious life-threatening injuries.

Note: Impact-level prioritization is used to identify those systems that may be of heightened interest or value to adversaries or represent a critical loss to the Federal enterprise, sometimes described as high value assets (HVAs).

SOs must:

1. Categorize information and the system in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

2. Ensure that the AO or AO's designated representative reviews and approves the security categorization decision; and

3. Document the security categorization decision in the security plan for the information system.

545.3.16.3 Risk Assessment (RA-3)

Effective Date: 12/28/2022

The CISO must:

a. Conduct a security and privacy risk assessment, including identifying threats to and vulnerabilities in the system, the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system, determining the likelihood and impact of adverse effects on individuals arising from the processing of PII, 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. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments.

d. Review risk assessment results at least annually and disseminate to the AO and system stakeholders.

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

545.3.16.4 Vulnerability Management and Scanning (RA-5)

Effective Date: 12/28/2022

Vulnerability management consists of detecting, assessing, and mitigating system weaknesses. Information sources include previous risk assessments, audit reports, vulnerability lists, security advisories, reports from public-at-large, 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 with tools that are Security Content Automated Protocol (SCAP)-validated and according to the ISCM Strategy.

b. Scan for vulnerabilities in the system and hosted applications in accordance with the **Continuous Vulnerability Assessment and Remediation Security Guidance** at least monthly, and when new vulnerabilities potentially affecting the system/applications are identified and reported (members of the USAID Workforce may contact **seceng@usaid.gov** to request access to the guidance document).

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

- Enumerating platforms, software flaws, and improper configurations;
- Formatting checklists and test procedures; and
- 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 system vulnerabilities to be scanned.

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

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

h. Define a **Vulnerability Disclosure Policy (VDP)** that provides guidance for the public and security researchers on where to submit vulnerability reports for USAID internet-accessible sites within policy scope (see **DHS BOD 20-01**). Vulnerability reports should be sent to M/CIO at **vdp@usaid.gov**.

SOs must:

1. Analyze vulnerability scan reports and results from security control assessments, and
2. Remediate legitimate vulnerabilities in accordance and in the timeframe identified by the associated risk impact level.

545.3.16.5 Risk Response (RA-7)

Effective Date: 12/28/2022

The CIO must provide procedures to respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Options for responding to risk include:

a. Mitigating risk by implementing new controls or strengthening existing controls;

b. Accepting risk with appropriate justification or rationale; and

c. Sharing, transferring, or avoiding risk.

The Agency's risk tolerance informs risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a POA&M entry. If the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a POA&M entry must be generated.

545.3.16.6 Privacy Impact Assessments (RA-8)
Effective Date: 12/28/2022

SOs must conduct PIA for systems or system components before:

a. Developing or procuring IT that processes PII; and

b. Initiating a new collection of PII that:

1. Will be processed using IT; and

2. Includes PII that permits the physical or virtual (online) contacting of a specific individual if identical questions have been posed to—or identical reporting requirements are imposed on—ten or more individuals, other than agencies, instrumentalities, or employees of the Federal Government.

For more details on how and when to conduct a PIA, see **ADS 508, section 508.3.4.3**.

545.3.16.7 Criticality Analysis (RA-9)
Effective Date: 12/28/2022

The CISO must identify critical system components and functions that require significant protections by performing a criticality analysis for all controls, including High Value Assets (HVAs), moderate systems, and system components supporting critical functions to the Agency mission.

A criticality analysis must be performed at least annually. It is recommended that an analysis be performed when a system's design or architecture is being developed, modified, or upgraded.

The criticality analysis identifies what organizational missions are supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware the hardware, software, and firmware components that implement those functions (supply chain risk analysis), including when the functions are shared by many components within and external to the system (*e.g.,* cloud instances).

545.3.17 System and Services Acquisition (SA)
Effective Date: 12/28/2022

The SA control family addresses security of information systems throughout a system's life cycle. It includes the acquisition of security tools and services and integrating security into requirements and processes early in the system development life cycle (SDLC).

545.3.17.1 Policy and Procedures (SA-1)

Effective Date: 12/28/2022

The Senior Procurement Executive (SPE) in the Bureau for Management, Office of Acquisition and Assistance (M/OAA) — in coordination with the Agency's CIO — must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency acquisition policy covering system and services that:

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;

b. Review the acquisition policy regularly and update as needed;

c. Develop, document, implement, and disseminate to system users procedures for system and services acquisition, to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls; and

d. Review system and services acquisition procedures at least annually and update as needed and following major changes.

545.3.17.2 Allocation of Resources (SA-2)

Effective Date: 12/28/2022

The Agency must allocate and identify resources for information security and privacy protection in the Agency's budget documentation.

For a system or system service either funded by program budget resources or OE budget resources or both, SOs must:

a. Identify high-level information security and privacy requirements for the system or system service in the planning process.

b. Determine, document, and allocate resources required to protect the system or system service as part of the Agency's Capital Planning and Investment control (CPIC) process. For additional information about the Agency's CPIC process,

see **ADS Chapter 509, Management and Oversight of Agency Information Technology Resources**. For more information on general Agency requirements on acquisition planning, see **USAID Acquisition Regulation [AIDAR]** and **ADS Chapter 300, Agency Acquisition and Assistance [A&A] Planning**.

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

The resources allocated for information security and privacy protection must include funding for acquisition, sustainment, and supply chain-related risks throughout the SDLC.

545.3.17.3 System Development Life Cycle (SA-3)

Effective Date: 12/28/2022

The Agency must develop and establish an SDLC process that integrates the organizational information security and privacy risk management process into SDLC activities (see **The USAID PMO Center of Excellence site** for information on the SDLC process).

SOs must manage their systems using the Agency SDLC process that incorporates information security and privacy considerations and must identify members of the workforce to perform information security and privacy roles and responsibilities throughout SDLC that are consistent with those identified in section **545.2, Primary Responsibilities**.

The incorporation of the security and privacy considerations in SDLC also requires SOs to:

a. Protect system pre-production environments commensurate with risk throughout the SDLC for the system, system component, or system service;

b. Approve, document, and control the use of live data in pre-production environments for the system, system component, or system service;

c. Protect pre-production environments for the system, system component, or system service at the same impact or classification level as any live data in use within the pre-production environments; and

d. Plan for and implement a technology refresh schedule for the system throughout the SDLC.

Security artifact templates assigned to each phase of the SDLC process are available for SO use (see the **SA&A Process** page for a link to security artifact templates).

545.3.17.4 Acquisition Process (SA-4)

Effective Date: 12/28/2022

The CO and the acquisition team must ensure that contracts for systems, system components, or system services include:

- Agency IT Security clauses (see **ADS 302mah**) and applicable FAR/AIDAR clauses;
- Security and privacy functional requirements;
- Strength of mechanism requirements;
- Security and privacy assurance requirements;
- Controls needed to satisfy the security and privacy requirements;
- Security and privacy documentation requirements;
- Requirements for protecting security and privacy documentation;
- Description of the system development environment and the environment in which the system is intended to operate;
- Allocation of responsibility or identification of parties responsible for information security, privacy, and SCRM; and
- Acceptance criteria.

In addition, the CO and the acquisition team must ensure contracts require the developer of the systems, system components, or system services to:

a. Provide a description of the functional properties of the security controls to be employed and the functions, ports, protocols, and services required, and 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;

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

c. Identify early in the SDLC the functions, ports, protocols, and services intended for organizational use;

d. 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. Note: Exceptions must be approved by M/CIO with input from the CISO;

e. 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 140-3**, when directed by the CISO or required by statute; and

f. Produce a plan for continuous monitoring of control effectiveness that is consistent with the Agency's continuous monitoring program.

In addition, contracts must:

1. Include the Agency's privacy requirements for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function (see section **545.3.15, Personally Identifiable Information Processing and Transparency (PT)** and **ADS 508** for additional information on the privacy requirements); and

2. Define data ownership requirements, specifically,

- Include organizational data ownership requirements in the contract, and
- Require all data to be removed from the contractor's system and returned to the organization within the Agency-defined timeframe.

For additional information on Agency development data requirements, see **ADS 579**. For information on the cloud computing acquisition process, see section **545.3.23.2, Cloud Computing**.

545.3.17.5 System Documentation (SA-5)

Effective Date: 12/28/2022

The CO and the acquisition team must ensure that contracts for systems, system components, or system services include requirements for the contractor to provide:

a. Administrator documentation for the systems, system components, or system services that describes:

- Secure configuration, installation, and operation of the systems, components, or services;
- Effective use and maintenance of security and privacy functions and mechanisms; and
- Known vulnerabilities regarding the configuration and use of administrative or privileged functions.

b. User documentation for systems, system components, or system services that describes:

- User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
- Methods for user interaction, which enables individuals to use the systems, components, or services in a more secure manner and protect individual privacy; and
- User responsibilities in maintaining the security of the systems, components, or services and privacy of individuals.

c. System documentation that is deemed sensitive to be labeled accordingly.

SOs must:

1. Ensure attempts to obtain documentation for systems, system components, or system services are documented when such documentation is either unavailable or nonexistent and appropriate actions are taken; and

2. Ensure the documentation is distributed to the administrator of the systems, security management personnel, and other personnel involved in the operation and maintenance of the systems, system components, or system services.

545.3.17.6 Security and Privacy Engineering Principles (SA-8)

Effective Date: 12/28/2022

Where applicable, SOs must ensure the following information security and privacy engineering principles are followed in the specification, design, development, implementation, and modification of the system and system components:

- Clear abstractions,
- Least common mechanism,
- Modularity and layering,
- Partially ordered dependencies,
- Efficiently mediated access,
- Minimized sharing,
- Reduced complexity,
- Secure evolvability,
- Trusted components,
- Hierarchical trust,
- Inverse modification threshold,
- Hierarchical protection,
- Minimized security elements,
- Least privilege,
- Predicate permission,

- Self-reliant trustworthiness,
- Secure distributed composition,
- Trusted communications channels,
- Continuous protection,
- Secure metadata management,
- Self-analysis,
- Accountability and traceability,
- Secure defaults,
- Secure failure and recovery,
- Economic security,
- Performance security,
- Human factored security,
- Acceptable security,
- Repeatable and documented procedures,
- Procedural rigor,
- Secure system modification,
- Sufficient documentation, and
- Minimization.

545.3.17.7 External System Services (SA-9)

Effective Date: 12/28/2022

SOs must:

a. Include the requirement that external information system services providers comply with organizational information security and privacy requirements in the contract 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 the control compliance by external service providers on an ongoing basis; and

d. Restrict the geographic location of information processing, information or data, and/or system services in support of Agency functions and based on a need to know.

SOs must also ensure that:

1. A risk assessment is conducted prior to the acquisition or outsourcing of information security services;

2. The acquisition or outsourcing of dedicated information security services is approved by the CISO;

3. Providers of applicable external system services identify the functions, ports, protocols, and other services required for the user of such services;

4. Appropriate actions are taken to verify that the interest of applicable external service providers are consistent with and reflect Agency interests;

5. The Agency maintains exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system;

6. The Agency has capability to check the integrity of information while it resides in the external system; and

7. The geographic location of information processing and data storage are restricted to facilities within the legal jurisdictional boundary of the United States unless an exception, *e.g.,* a Google data center located overseas, is approved by the AO.

545.3.17.8 Developer Configuration Management (SA-10)
Effective Date: 12/28/2022

SOs must:

a. Approve all changes to the system; and

b. Include, in the contract, the requirement for developers of information systems to provide and follow an approved configuration management plan during development and operation, at a minimum. 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,

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

    4. Ensure that appropriate security and privacy representatives are included in the configuration change management and control process.

545.3.17.9 Developer Testing and Evaluation (SA-11)
Effective Date: 12/28/2022

SOs must include the requirements for the developer of the systems, system components, or system services in contracts at all post design stages of the SDLC to:

a. Create and implement a security assessment plan;

b. Perform 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's business needs;

c. Produce supporting evidence and the results of the security and privacy testing/evaluation;

d. Employ interactive application security testing tools to identify flaws and document the results;

e. Implement a verifiable flaw remediation process;

f. Correct flaws identified during security and privacy testing/evaluation; and

g. Test critical software in a manner consistent with the **NIST Guidelines on Minimum Standards for Developer Verification of Software**.

545.3.17.10 Development Process, Standards, and Tools (SA-15)

Effective Date: 12/28/2022

SOs must include in contracts the requirements for the developer of the systems, system components, or system services to:

a. Follow a documented development process that:

- Explicitly addresses security and privacy requirements;
- Identifies the standards and tools used in the development process;
- Documents the specific tool options and tool configurations used in the development process; and
- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.

b. Review the development process, standards, tools, tool options, and tool configurations annually to determine if they satisfy the USAID's security and privacy requirements.

Where applicable, SOs must require the developer of systems, system components, or system services to:

1. Define quality metrics at the beginning of the development process and provide evidence of meeting the quality metric upon the delivery;

2. Select and employ security and privacy tracking tools for use during the development process;

3. Perform a criticality analysis at the appropriate decision points in SDLC at key points in the SDLC cycle, and at the appropriate level of rigor;

4. Reduce attack surfaces;

5. Implement an explicit process to continuously improve the development process;

6. Perform an automated vulnerability analysis using appropriate tools, determine the exploitation potential for discovered vulnerabilities, determine potential risk mitigations for delivered vulnerabilities, and deliver the outputs of the tools and results of the analysis to SOs;

7. Use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process;

8. Provide, implement, and test an IRP;

9. Archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review; and

10. Minimize the use of PII in development and test environments.

545.3.17.11 Unsupported System Components (SA-22)
Effective Date: 12/28/2022

SOs must:

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Use in-house resources or find alternative contractors to support the system components.

545.3.18 System and Communications Protection (SC)
Effective Date: 12/28/2022

The SC control family provides security safeguards for a system, including the confidentiality and integrity of data at rest and in transit, separating user functionality and system management functionality, and establishing boundary protections to monitor and control communications.

545.3.18.1 Policy and Procedures (SC-1)
Effective Date: 12/28/2022

The CISO must:

a. Develop, document, implement, and disseminate to the USAID workforce an

Agency system and communications protection policy that:

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Review the system and communications protection policy annually and update as needed.

c. Designate a policy lead to manage the development, documentation, and dissemination of the system and communications protection policy.

SOs must:

1. Develop, document, implement, and disseminate to users system and communications protection procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

2. Review system and communications protection procedures at least annually and update, as needed, and following major system changes.

545.3.18.2 Separation of System and User Functionality (SC-2)
Effective Date: 12/28/2022

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

545.3.18.3 Information in Shared System Resources (SC-4)
Effective Date: 12/28/2022

SOs must configure the system to prevent the unauthorized or unintended sharing of information—either unauthorized or unintended—via shared system resources. Use of reusable electronic media must follow CISO guidance during its life cycle.

545.3.18.4 Denial-of-Service Protection (SC-5)
Effective Date: 12/28/2022

SOs must ensure that systems, including wireless devices and endpoints, limit the effects of internal and external denial of service attacks by employing M/CIO- and CISO-approved safeguards such as load balancers, packet filtering devices, capacity planning, and resource allocation monitoring.

545.3.18.5 Boundary Protection (SC-7)
Effective Date: 12/28/2022

SOs must ensure the information systems will align with the CIO Zero Trust Network Architecture and will be configured to:

a. Monitor and control communications at the externally managed interfaces to the system and at key internally managed interfaces 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 systems only through managed interfaces consisting of CISO-approved boundary protection devices arranged in accordance with CIO security and privacy architecture that limits the number of external network connections to the system;

d. Implement managed interfaces for each external telecommunications 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 the 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. Filter DNS spoofing and any threatening outgoing communications traffic from external networks;

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

k. Prevent remote devices from simultaneously establishing non-remote connections with the system and communicating through some other connection to resources in external networks;

l. Prevent the exfiltration of information by inspection and by blocking techniques implemented at internal endpoints, data loss prevention solutions, external boundaries, and managed interfaces; and

m. Implement host-based boundary protection in servers, laptops, and mobile

devices.

545.3.18.6 Transmission Confidentiality and Integrity (SC-8)
Effective Date: 12/28/2022

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

The system implements cryptographic mechanisms to prevent unauthorized disclosure and detects changes to information during transmission unless otherwise protected by written CISO-approved mechanisms.

545.3.18.7 Network Disconnect (SC-10)
Effective Date: 12/28/2022

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

545.3.18.8 Cryptographic Key Establishment and Management (SC-12)
Effective Date: 12/28/2022

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

545.3.18.9 Cryptographic Protection (SC-13)
Effective Date: 12/28/2022

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

545.3.18.10 Collaborative Computing Devices and Applications (SC-15)
Effective Date: 12/28/2022

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

If remote activation or use is authorized, SOs must ensure the 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.

545.3.18.11 Public Key Infrastructure Certificates (SC-17)
Effective Date: 12/28/2022

SOs must only issue public key certificates or use public key service providers that are authorized and approved by the CIO and CISO. SOs must only include approved trust anchors in trust stores or certificate stores managed by the M/CIO.

545.3.18.12 Mobile Code (SC-18)
Effective Date: 12/28/2022

The CISO must define acceptable and unacceptable usage policies for mobile code and mobile code technologies. The policies must authorize, monitor, and control the use of mobile code within the system. SOs must identify unacceptable mobile code and take the necessary corrective action when such code is detected.

545.3.18.13 Secure Name/Address Resolution Service (Authoritative Source) (SC-20)
Effective Date: 12/28/2022

SOs must configure the 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 Domain Name Service 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, 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 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 M-08-23**.

545.3.18.14 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21)
Effective Date: 12/28/2022

SOs must ensure that the 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. For more information, see **OMB Memorandum M-08-23**.

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

Effective Date: 12/28/2022

SOs must ensure that systems that collectively provide name/address resolution services for an organization are fault-tolerant and implement internal/external role separation.

545.3.18.16 Session Authenticity (SC-23)

Effective Date: 12/28/2022

SOs must ensure that systems protect the authenticity of communications sessions by using CISO-approved TLS certificates, MFA, and layers that ensure sessions are between trusted resources to prevent threats.

545.3.18.17 Protection of Information at Rest (SC-28)

Effective Date: 12/28/2022

SOs must protect the confidentiality and integrity of all data-at-rest residing in FISMA moderate systems or any system containing PII or SBU information, including databases and cloud services. SOs must implement cryptographic mechanisms for Moderate impact systems to prevent unauthorized disclosure and modification of the information at rest.

- Mobile devices and laptops must be protected with **FIPS 140-3** or later compliant encryption;
- Databases must be protected with transparent data (TDE) encryption or equivalent running in FIPS mode; and
- Systems hosted in the Cloud must meet the minimum **Federal Risk and Authorization Management Program (FedRAMP)** requirements.

545.3.18.18 Process Isolation (SC-39)

Effective Date: 12/28/2022

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

545.3.19 System and Information Integrity (SI)

Effective Date: 12/28/2022

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

545.3.19.1 Policy and Procedures (SI-1)
Effective Date: 12/28/2022

The CISO must:

a. Develop, document, implement, and disseminate to USAID workforce members with a need to know an Agency system and information integrity policy that:

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Review the system and information integrity policy annually and update as needed and following major system changes.

c. Designate a policy lead to manage the development, documentation, and dissemination of the system and information integrity policy.

SOs must:

1. Develop, document, implement, and disseminate to users system and information integrity procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

2. Review system and information integrity procedures at least annually and update as needed and following major system changes.

545.3.19.2 Flaw Remediation (SI-2)
Effective Date: 12/28/2022

M/CIO must employ automated mechanisms that scan at least weekly and when required by the CISO to determine the state of system components on flaw remediation.

SOs must:

a. Identify and report flaws with the support of ISSOs and SOC, and centrally manage the flaw remediation process to correct system flaws;

b. Test software and firmware 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;

d. Install security-relevant software and firmware updates within timelines defined in the Continuous Vulnerability Assessment and Remediation Security Guidance; and

e. In coordination with SOC, prevent devices or applications with critical flaws that pose a threat to the Agency from connecting or operating within Agency networks until remediation is complete.

545.3.19.3 Malicious Code Protection (SI-3)

Effective Date: 12/28/2022

M/CIO must implement, centrally manage, and automatically update, when possible, (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. Periodic or continuous scans of the 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 that block or quarantine malicious code and send alerts in response to malicious code detection.

SOs, in coordination with the Security Operations Center (SOC), must address the receipt of false positives during malicious code detection and eradication and the resulting impact on the availability of the system.

SOs must:

1. Implement adequate signature based and/or non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

2. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.

3. Configure malicious code protection mechanisms to:

- Perform periodic and continuous scans of the system and real-time scans of files from external sources at endpoint, network entry, and/or exit points as the files are downloaded, opened, or executed in accordance with organizational

policy; and

- Take appropriate action to block and/or quarantine malicious code, and alert the **cio-helpdesk@usaid.gov** and incident response team in response to malicious code detection; and

4. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

545.3.19.4 System Monitoring (SI-4)

Effective Date: 12/28/2022

SOs, with the support of ISSOs and the SOC, must monitor events on systems to detect and identify indicators of potential attacks, 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 **Cybersecurity Log, Event, and Audit Standards** (to obtain copies of these documents, email **ato@usaid.gov**).

SOs must:

a. Invoke internal monitoring capabilities and/or deploy monitoring devices strategically within the system to collect organization-determined essential information;

b. Analyze detected events and anomalies;

c. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

d. Obtain legal opinion regarding system monitoring activities (all information is protected under the Privacy Act of 1974 and in accordance with **ADS 508**);

e. Provide audit logs to a SIEM enterprise system, ISSOs, and the CISO, as needed;

f. Ensure the system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions;

g. Ensure the system alerts ISSOs and SOC when indications of compromise or potential compromise occur; and

h. Coordinate with the CISO to ensure the system has a capability to address, discover, collect, distribute, and use indicators of compromise.

M/CIO must:

1. Deploy monitoring devices at ad hoc locations within M/CIO managed systems to track specific types of transactions of interest to the Agency;

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 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.

545.3.19.5 Security Alerts, Advisories, and Directives (SI-5)

Effective Date: 12/28/2022

The CISO must:

a. Receive 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 the USAID workforce and 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.

545.3.19.6 Software, Firmware, and Information Integrity (SI-7)

Effective Date: 12/28/2022

M/CIO must employ integrity verification tools to detect unauthorized changes or modifications to mission critical or security related 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.

545.3.19.7 Spam Protection (SI-8)

Effective Date: 12/28/2022

M/CIO must deploy and centrally manage an enterprise spam protection mechanism.

SOs must:

a. Employ or ensure spam protection mechanisms at 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. System entry and exit points include, but are not limited to, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

545.3.19.8 Information Input Validation (SI-10)
Effective Date: 12/28/2022

SOs must ensure that the system checks the validity of SO-defined input values. Input validation helps to ensure accurate and correct inputs and prevent attacks (*e.g.,* cross-site scripting and a variety of injection attacks).

545.3.19.9 Error Handling (SI-11)
Effective Date: 12/28/2022

SOs must ensure that the 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 members of the workforce.

545.3.19.10 Information Management and Retention (SI-12)
Effective Date: 12/28/2022

SOs must manage and retain information within a system and the output from the system in accordance with **ADS 502** and section **545.3.11, Media Protection**.

545.3.19.11 Memory Protection (SI-16)
Effective Date: 12/28/2022

SOs must implement controls to protect system memory from unauthorized code execution. Ensuring the system implements hardware or software enforced data execution prevention safeguards to protect its memory from unauthorized code execution.

545.3.19.12 Personally Identifiable Information Quality Operations (SI-18)
Effective Date: 12/28/2022

SOs must check the accuracy, relevance, timeliness, and completeness of PII across the information life cycle at least annually and correct or delete inaccurate or outdated PII to correct or delete PII that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.

See **ADS 578, Information Quality Guidelines**, and **ADS 597sad, Data Quality Assessment Checklist,** and **ADS 508 section 508.3.5.6** for more information about data quality.

545.3.19.13 De-identification (SI-19)
Effective Date: 12/28/2022

SOs must:

a. At a minimum, remove the following elements of PII from datasets prior to publicly releasing data: name (first and last), social security number (to include last four), date of birth, mother's maiden name, and biometric records.

Note: Removing direct identifiers only may not be sufficient for certain disclosures and/or release models. de-identify. Decisions about how to de-identify data are based on how the data are used, processed, stored and shared (see **NISTIR 8053, De-Identification of Personal Information for more information**).

b. Evaluate the effectiveness of de-identification at least annually.

Releases should be monitored by the data owners who authorized the data release to assure that the assumptions made during the de-identification remain valid.

See **ADS 579, Development Data** and **ADS 508** for more information about the process for releasing and publishing USAID data.

545.3.20 Supply Chain Risk Management (SR)
Effective Date: 12/28/2022

The SR control family addresses the organizational risks associated with external system dependencies and how to control and verify them. SR controls cover cloud and third party services and systems and include creation of a supply chain risk management plan, critical supply chain process, and conduct of regular assessments and supplier reviews.

545.3.20.1 Policy and Procedures (SR-1)
Effective Date: 12/28/2022

The CIO must:

a. Develop, document, implement, and disseminate to the USAID workforce an Agency supply chain risk management (SCRM) policy that:

- Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

b. Review the SCRM policy annually and update as needed and following breaches or identified compromises of Agency supply chains, as necessary.

c. Develop, document, implement, and disseminate to the USAID workforce an SCRM procedures to facilitate the implementation of the SCRM policy and the associated SCRM controls; and

d. Review SCRM procedures at least annually and update as needed following breaches or identified compromises of Agency supply chains.

The Agency must designate a Senior Agency Official for Supply Chain Risk Management (SAO-SCRM) to manage the development, documentation, and dissemination of the SCRM policy.

545.3.20.2 Supply Chain Risk Management Plan (SR-2)

Effective Date: 12/28/2022

The USAID SAO-SCRM must:

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of all systems, system components, and system services;

b. Review and update the SCRM plan annually (or as required) to address threat, organizational, or environmental changes; and

c. Protect the SCRM plan from unauthorized disclosure and modification.

The SAO-SCRM will establish a supply chain risk management team consisting of the members of the SCRM Working Group (*i.e.,* M/CIO, GC, OAA, and SEC leadership) to lead and support the following SCRM activities:

1. Develop an Agency-wide Information and Communications Technology (ICT) SCRM strategy;

2. Establish an approach to identify and document Agency ICT supply chains;

3. Establish and mature an interactive process to conduct Agency-wide assessments of ICT supply chain risks;

4. Establish a process to conduct reviews of potential suppliers prior to selecting ICT products and services;

5. Develop ICT SCRM requirements for inclusion in contracts that are tailored to the type of contract and business needs; and

6. Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment.

545.3.20.3 Supply Chain Controls and Processes (SR-3)

Effective Date: 12/28/2022

The SAO-SCRM must:

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of all Agency systems in coordination with the ICT SCRM committee.

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events:

- Integrate representatives from multiple functions within the Agency into one larger supply chain program,
- Establish an enterprise-wide supply chain risk management program, and
- Identify supplier evaluation criteria that would reduce or mitigate the impact of the threat.

c. Implement cyber-hygiene practices to monitor and mitigate the supply chain risk.

d. Document the selected and implemented supply chain processes and controls in the SCRM Strategy.

545.3.20.4 Acquisition Strategies, Tools, and Methods (SR-5)

Effective Date: 12/28/2022

The SAO-SCRM must employ acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks in accordance with contracting policy and purchase card guidance (see **ADS 300**, **ADS 302**, **ADS 331** and relevant FAR clauses).

545.3.20.5 Supplier Assessments and Reviews (SR-6)
Effective Date: 12/28/2022

The SAO-SCRM must assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide annually.

545.3.20.6 Notification Agreements (SR-8)
Effective Date: 12/28/2022

The ICT SCRM program was developed to establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises and the results of assessments or audits.

545.3.20.7 Inspection of Systems and Components (SR-10)
Effective Date: 12/28/2022

The ICT SCRM program was developed to establish the inspection of a sample of systems and spot check a set of system components annually upon acquisition of new system components to detect tampering.

545.3.20.8 Component Authenticity (SR-11)
Effective Date: 12/28/2022

The SAO-SCRM must:

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Require SOs to report identified counterfeit system components to the SCRM team.

The SAO-SCRM must ensure that:

1. SCRM team members are trained to detect counterfeit system components (*e.g.,* hardware, software, and firmware); and

2. Configuration control is maintained over system components awaiting service or repair and serviced or repaired components awaiting return to service on all Agency systems and system components.

545.3.20.9 Component Disposal (SR-12)
Effective Date: 12/28/2022

The CISO must dispose of Agency data, documentation, tools, or system components in accordance with the **NIST SP 800-88 Revision 1, Guidelines for Media**

Sanitization.

545.3.21 Other USAID-Specific Policies

545.3.21.1 Acceptable Use
Effective Date: 12/28/2022

M/CIO established an acceptable use policy and the potential referral for disciplinary actions for misuse of IT resources—including email, Internet, and Intranet. The Agency must ensure that the USAID workforce uses 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, Agency-wide ROB, agreements, standards, checklists, and guidelines derived from this policy (see **ADS 545mam, Acceptable Use Policy for IT Resources**; **ADS 547**; **ADS 549**; and **ADS 545mbd**).

b. The workforce must adhere to the M/CIO, ROB policy on the acceptable use of 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, except in an emergency or exceptional circumstance (see **ADS 502**). The following policy statements apply to the use of electronic messaging accounts:

- Non-official electronic messaging (*e.g.,* personal Gmail and Yahoo, and email accounts ending in .com, .net, .org, among others) 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 (*e.g.,* flood or tornado), a national security event, or a regional power loss of six hours or more (see **ADS 502**).

- 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 workforce 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. The requestor must submit the waiver request to the M/CIO CISO.

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, or there are exceptional circumstances. This policy is enforceable under Federal law and violators may be prosecuted.

- Work must follow the standards and procedures outlined in **ADS 545mam**.

- 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 that do not contain USAID SBU manually.

- In accordance with the **Cybersecurity Act of 2015** and **OMB Circular A-130, Managing Information as a Strategic Resource**, Federal agencies must encrypt sensitive and mission-critical data that is stored on Agency information systems or is transmitted to or from information systems to prevent access by unauthorized users. This means that all email attachments containing PII must be encrypted, whether the recipient is inside or outside USAID. This guidance also applies to emails exchanged between two .gov or .mil email accounts (see the **Cybersecurity Act of 2015 [P. L. 114-113, Division N]** and the **Agency Notice, "Mandatory Encryption of Email Attachments Containing PII"**).

d. Workforce members 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 (*e.g.,* pornography).

e. Workforce members must protect PII and sensitive information to the greatest extent feasible in accordance with this policy and Federal laws. PII is protected under the Privacy Act of 1974 and in accordance with ADS 508 and OMB A-130.

f. Workforce members have no expectation of privacy when using government resources. All equipment operated on behalf of USAID is subject to monitoring in accordance with this policy (see section **545.3.19.4, System Monitoring [SI-4])**; however, all PII is protected under the **Privacy Act of 1974** and in accordance with **ADS 508**).

g. Workforce members must ensure that intellectual property is handled and

managed in accordance with USAID license rights to such intellectual property. Intellectual property is intangible property, such as patents, trademarks, and copyrighted materials, which are the result of intellectual effort and are under legal protection. Workforce members using, storing, or distributing copyrighted materials on a USAID information system must ensure the copyright notice is clearly included with the material and that USAID has rights to the material. Consultation with GC/RLO on the use of copyrighted materials is required (see ADS 318).

Workforce members requiring access to a USAID system must follow agency procedures for access. Workforce members requiring access to USAID sensitive or proprietary information must have a need to know the information in order to perform the duties of their position and, in some circumstances, may be asked to sign a data use agreement or Non-Disclosure Agreement (NDA) (note: Agency workforce must vet any custom NDA with GC for legal sufficiency).

545.3.21.2 Information Security Policy Violation and Disciplinary Action
Effective Date: 12/28/2022

Members of the workforce who commit policy infractions, intentional or unintentional, including misuse of USAID IT resources, may be referred for disciplinary actions as defined in **ADS Chapter 485, Disciplinary Action - Foreign Service** or **ADS Chapter 487, Disciplinary and Adverse Actions Based Upon Misconduct - Civil Service**. These disciplinary actions may include removal.

Contractor employees may have their access privileges revoked and the contract itself could be terminated as a result of an infraction.

In addition to disciplinary action, workforce members may be required to complete remedial training and may have their access privileges revoked.

When such actions appear to be criminal in nature, the matter must be referred to the USAID Office of the Inspector General (OIG).

545.3.21.3 Requirement to Connect Laptops to AIDNet Every 30 Days
Effective Date: 12/28/2022

All GFE laptops must be connected to AIDNET every 30 days to maintain a minimum healthy state. Devices not in compliance present a threat to the security posture of USAID networks and will be denied access to AIDNet.

In scenarios where users are not able to connect to AIDNet (*e.g.,* permanent telework, extended TDY, etc.), M/CIO has deployed a technical solution enabling laptops that are not connected to AIDNet to receive security patches when connected to the Internet via Wi-Fi or when hard wired. In these instances, users must connect their laptops to the internet every 30 days in order for patches to be installed.

See **ADS 549** for guidance on connecting mobile phones to a cellular/data network

every 30 days.

545.3.21.4 Elevated Privilege Account Usage Limitations
Effective Date: 12/28/2022

An elevated privilege user is a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. Workforce members with elevated privilege accounts (*e.g.,* SOs, system administrators, ISSOs, system managers, etc.) must only use these accounts to perform administrative functions required by their position. For example, they must not use their elevated privilege account to access the Internet, perform administrative activities outside of VDI (https://remoteaccess.usaid.gov), create unauthorized accounts, send personal messages, or access personal accounts, etc.

Workforce members must use their regular user accounts to perform all other tasks (*e.g.,* checking email, accessing the Internet). Please contact **seceng@usaid.gov** with any questions.

Misuse of elevated privilege may result in revocation of privileged access, revocation of security clearance, and/or disciplinary actions.

545.3.22 Prohibited and Restricted Use Technologies
Effective Date: 12/28/2022

USAID prohibits or restricts certain activities and the use of certain technologies that introduce threats or exceptionally high risks to the Agency (see **ADS 545mam** for more information).

545.3.22.1 Social Media and Social Networking
Effective Date: 12/28/2022

Social media sites can be internally hosted/developed solutions or hosted by external commercial services and 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 Chapter 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 authorization to operate (ATO), risk decision memorandum based on a risk assessment, and/or M/CIO security assessment report.

Note: Refer to section **545.3.13.3, Rules of Behavior (PL-4)** 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. Workforce members must not post sensitive information, to include PII, on a social media website unless the **Privacy Act** and the **Freedom of Information Act** (FOIA) permit release of the information (see **ADS 507** for USAID FOIA guidance). In advance of the release of PII, members of the workforce must consult with the CPO. In advance of the release of sensitive information members of the workforce must consult with the FOIA Officer.

d. SOs, CORs, or others responsible for Agency social media/networking applications must ensure via contracts or other agreements that records are retained consistent with the Agency records retention requirements (see **ADS Chapter 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 workforce members assigned responsibility for operating an official account or contributing to a social media website:

1. Workforce members 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. SOs must obtain approval from GC for a cloud service provider's Terms of Service (ToS) agreement as a condition of use. M/CIO must verify GC approval prior to authorizing use.

3. Workforce members must not post any official Agency positions on social media sites unless explicitly authorized by LPA. This does not include sharing or reposting official Agency positions.

4. Workforce members 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. Social Media Account Managers must review the appropriate ToS for the social media platform.

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 understand 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. Social media postings that put workforce members in direct contact with the public (*i.e.,* comment, engage) must be carefully vetted with the Development Outreach Coordinator in Missions, with B/IO leadership, and with LPA in USAID/W (when appropriate), before responding to comments.

545.3.23 Other Technologies

545.3.23.1 Third-Party Websites

Effective Date: 12/28/2022

Third-party websites are sites funded by the Agency, hosted on environments external to USAID boundaries, and not directly controlled by USAID policies and workforce members, except through the terms and conditions of contracts, grants, or cooperative agreements (see **ADS Chapter 557, Public Information**). The following policies apply to these websites:

a. Approval. All third-party websites must be evaluated and approved by the LPA Website Governance Board (**webgovernanceboard@usaid.gov**) prior to site development.

b. Development. All third-party websites, once approved to be developed, are subject to additional review and approval by the USAID Office of the CIO (M/CIO). The review and approval can include, but is not limited to, compliance with applicable federal mandates, policies and executive orders, continuous monitoring, vulnerability remediation and proper disposal, decommissioning and/or archiving of the website at the end of the contract period of performance in compliance with record retention policies established by the Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD).

c. Third-Party Privacy Policies. For guidance on Third-Party Privacy Policies, please see **ADS 508**.

d. External Links. Posting a link to a third-party website 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 website where the privacy policies might be different.

e. Embedded Applications. Incorporating or embedding a third-party application on a

USAID website or in any other government domain requires disclosing the third-party's involvement and describing the Agency's Privacy Policy (*i.e.,* **ADS 508**).

f. Information Collection. Regarding the use of third-party websites 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**).

545.3.23.2 Cloud Computing

Effective Date: 12/28/2022

Cloud computing is a model for enabling convenient and on-demand network access to a shared pool of configurable computing resources. These resources 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 systems must:

1. Comply with the FedRAMP Security Assessment Framework; or

2. Be assessed by USAID in accordance with NIST SP 800-53 Rev 5 requirements. For more information, see the cloud systems documentation on the **SA&A Process** page.

b. The SO and/or COR must coordinate with the CO and M/CIO to ensure 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** include requirements for:

- Regulatory compliance (*i.e.,* 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 by or on behalf of USAID 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**.

545.3.23.3 Applications or Services Sending Emails Using USAID.gov Email Address

Effective Date: 12/28/2022

Any application or service that sends email using a USAID.gov email address (*e.g.,* services like Constant Contact, MailChimp, or ServiceNow) must be authorized through M/CIO to send email on behalf of the Agency and must comply with Department of Homeland Security (DHS) **Binding Operational Directive (BOD) 18-01, Enhance E-mail and Web Security**.

To request authorization to send emails as "@usaid.gov," open a ticket with the M/CIO Service Desk at **cio-helpdesk@usaid.gov**. Failure to do so may flag your email as spam or your email may be rejected by the Agency's firewalls.

545.3.24 Waivers

Effective Date: 12/28/2022

A waiver is the written permission required to temporarily or permanently eliminate the requirements of a specific policy or control outlined in this policy chapter. For ADS 545, an SO might consider requesting a waiver for a legacy or end-of-life system for which full compliance with some portion of the policy is not cost effective. Alternatively, an SO

may determine that implementing a specific security control would negatively affect a critical Mission function to a level they deem to be unacceptable.

A waiver is granted only in exceptional cases and is not intended to serve as a remedy for systems that have not followed the required process to obtain an ATO. In all cases, an SO must attempt to implement the minimum necessary controls as outlined by NIST and M/CIO defined compensating controls. When a system cannot be made to fully comply with policy and regulatory requirements due to a business need, the SO must request a waiver in writing from the CISO. The CISO will approve or disapprove the waiver based on an assessment of the risk to the Agency of the system's non-compliance.

545.4 MANDATORY REFERENCES

545.4.1 External Mandatory References

Effective Date: 03/28/2023

a. 5 Code of Federal Regulations (CFR) Part 731.106, Designation of Public Trust Positions and investigative Requirements, January 2012

b. 5 CFR Part 2635.704, Use of Government Property (as amended at 81 FR 81641) January 1, 2017

c. 12 FAM 540, Sensitive But Unclassified Information (SBU)

d. Agency for International Development Acquisition Regulation (AIDAR)

e. Binding Operational Directives (BODs) and Emergency Directives (EDs), issued by the U.S. Department of Homeland Security

f. Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service, Chief Acquisition Officers Council/Federal Cloud Compliance Committee, February 24, 2012

g. EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011

h. Federal Information Processing Standards (FIPS) 140-3, Security Requirements for Cryptographic Modules, March 22, 2019

i. FIPS 197, Advanced Encryption Standard (AES), November 26, 2001

j. FIPS-199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

k. FIPS 201, Personal Identity Verification (PIV) of Federal Employees and

Contractors

l. Foundations for Evidence-Based Policymaking Act of 2018 **(Evidence Act)**

m. Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003

n. HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004 (Authority)

o. John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019, August 13, 2018

p. National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience

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

r. 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)

s. NIST SP 800-18 Rev 1, Guide for Developing Security Plans for Information Technology Systems, February 2006

t. NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations, December 2018

u. NIST SP 800-39, Managing Information Security Risk, March 2011

v. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002

w. NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020

x. NIST SP 800-53A, Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, December 2014 *(awaiting release of Rev 5)*

y. NIST SP 800-55, Rev. 1, Performance Management Guide for Information Security, July 2008

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

aa. NIST SP 800-63, Digital Identity Guidelines, June 2017

ab. NIST SP 800-88, Rev. 1, Guidelines for Media Sanitization, December 2014

ac. NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems

ad. NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011

ae. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011

af. NIST SP 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials, December 2014

ag. NIST 1800-12, Derived PIV Credentials Practice Guide, 2019

ah. NIST Description, The United States Government Configuration Baseline (USGCB), March 7, 2010

ai. OMB Circular No. A-130, July 2016

aj. OMB Cyber Spend Reporting Requirements/Budget Data Requests (BDR)

ak. OMB Enterprise Architecture Assessment Framework

al. OMB Memorandum 08-23, Securing the Federal Government's Domain Name System Infrastructure, August 23, 2008

am. OMB Memo M-04-16, Software Acquisition, July 1, 2004

an. OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, May 21, 2019

ao. OMB Memorandum M-19-18, Federal Data Strategy - A Framework for Consistency, June 4, 2019

ap. OMB Memorandum M-19-23, Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Leaming Agendas, Personnel, and Planning Guidance, July 10, 2019

aq. OMB Memorandum M-20-04, Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements, November 19, 2019

ar. OMB Memorandum M-22-13, "No TikTok on Government Devices" Implementation Guidance

as. P. L. 113-283, Federal Information Security Modernization Act of 2014 (FISMA), December 8, 2014

at. P. 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)

au. P.L. 117-328, The Consolidated Appropriations Act, 2023

av. U.S. Department of Homeland Security Binding Operational and Emergency Directives

545.4.2 Internal Mandatory References

Effective Date: 12/28/2022

a. ADS 103, Delegations of Authority

b. ADS 302, USAID Direct Contracting

c. ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology

d. ADS 331, USAID Worldwide Purchase Card Program

e. ADS 485, Disciplinary Action - Foreign Service

f. ADS 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct - Civil Service

g. ADS 501, The Automated Directives System

h. ADS 502, The USAID Records Management Program

i. ADS 502mab, Strategic Objective Document Disposition Schedule

j. ADS 507, Freedom of Information Act (FOIA)

k. ADS 508, Privacy Program

l. ADS 509, Management and Oversight of Agency Information Technology Resources

m. ADS 519, Building Support Services in USAID/Washington

n. ADS 545mam, Acceptable Usage Policy for Information Technology Resources

o. ADS 545mau, Password Creation Standards

p. ADS 545mbd, Rules Of Behavior for Users

q. ADS 545mbg, Wireless Standards and Guidelines

r. ADS 547, Property Management of Information Technology (IT) Resources

s. ADS 549, Telecommunications Management

t. ADS 552, Cyber Security for National Security Information (NSI) Systems

u. ADS 557, Public Information

v. ADS 558, Use of Social Media For Public Engagement

w. ADS 562, Physical Security Programs (Overseas)

x. ADS 565, Domestic Security Programs

y. ADS 566, Personnel Security Investigations and Clearances

z. ADS 569, Counterintelligence Program

aa. ADS 579, USAID Development Data

ab. ADS 596, Management's Responsibility for Internal Control

ac. M/CIO Strategic Planning and Enterprise Architecture

545.5 ADDITIONAL HELP

Effective Date: 12/28/2022

a. IDmanagement.gov

545.6 DEFINITIONS

Effective Date: 12/28/2022

See the ADS Glossary for all ADS terms and definitions.

802.11
The numbering refers to a protocol 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 from a few meters to more than 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 on the agreed upon implementation of a prescribed set of security controls. (**Chapter 545**)

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

Advanced Encryption Standard (AES)
Products using **FIPS 197, Advanced Encryption Standard (AES)** algorithms with at least 256-bit encryption validated under **FIPS 140-3**, 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 (*i.e.,* both an installed instance and a physical instance), virtual computing platform, and related hardware (*e.g.,* locks, cabinets, keyboards). (NISTIR 7693, Specification for Asset Identification 1.1 [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**)

Authorization 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 or 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 workforce members' understanding of the importance of security and the adverse consequences of its failure. Training activities teach members of the workforce the skills to perform their jobs more effectively. Educational activities are more in-depth than training. (Source: **NIST SP 800-12, Rev. 1, An Introduction to Information Security**) (**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**)

Bureau for Humanitarian Assistance (BHA)
An organizational unit within USAID that directs and coordinates international United States Government disaster assistance. (**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, Business, or Information Owner (IO). In general, BOs ensure that the mission of the organization is accomplished. In some cases, BOs 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. (**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 used 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 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 system's 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)
An effort within individual organizations to ensure they can continue to perform their essential functions during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. (**Chapters 405, 511, 524, 531, 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**) (**Chapter 545**)

Critical Threat Mission/Post
This term refers to those Missions/posts that are defined by the DoS 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**)

Cyber-Physical
A system that includes engineered, interacting networks of physical and computational components. **(NIST SP 800-160 Vol. 1)**

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (Source: **OMB Circular No. A-130**)

Dedicated Machine
A machine exclusively used for a single purpose (*i.e.,* 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)
DATO is determined when the Agency Authorizing Official (AO) (*i.e.,* the CIO), 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 an 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; 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 (i.e., to accredit) an automated information system (i.e., major application or GSS) and accept the risk associated with the system. (Source: **NIST SP 800-12, Rev. 1**) (**Chapter 545**)

Development Environment
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 the USAID critical business functions that are handled by its information systems are resumed and restored after a natural or manmade 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. The server performs this service 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
Includes all USAID direct-hire personnel and personal service contractors. (**Chapters 110, 331, 410, 443, 450, 457, 514, 545, 621, 625**)

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 to support USAID. (**Chapter 545**)

Executive Officer (EXO)
The Unit Security Officer, responsible to both SEC and the post RSO, ensures Agency compliance with USAID and post security directives. (**Chapter 545**)

Executive Order (E.O.)
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, and operated or owned by the Agency. These are systems under contract to, funded by, and operated on behalf of the Agency. (**Chapter 545**)

Federal Acquisition Regulation (FAR)
The primary document that contains the uniform policies and procedures for all executive agencies for the acquisition of supplies and services with Congressional appropriations. It is Chapter 1 of **Title 48, Code of Federal Regulations (CFR)**. (**Chapters 300, 302, 331, 545**)

Federal Desktop Core Configuration (FDCC)
A list of security settings recommended by NIST for general-purpose microcomputers connected directly to the network of a U.S. 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 U.S.C. § 3541, et seq.), a U.S. Federal law enacted in 2002 as Title III of the E-Government Act of 2002 (P. 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 U.S.C. § 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 OMB and DHS for information security. It also updates guidelines that Federal agencies should follow in the event 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
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 to 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)
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 U.S. 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, is largely uncontrolled and proprietary (i.e., not subject to source review), and as a result might contain malicious code. (**Chapter 545**)

Functional or Program Managers (PMs)

A subclass of users that, in some cases, 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 U.S. government established in 1949 to help manage and support the basic functioning of Federal agencies. GSA supplies products and communications for U.S. Government offices, provides transportation and office space to Federal employees, develops government-wide cost-minimizing policies, and performs 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 a shared information processing service organization. (Source: **OMB Circular No. A-130**) (**Chapter 545**)

Government Information Security Reform Act (GISRA)
Enacted in 2000 and replaced by FISMA in 2002, this Federal law required U.S. Government agencies to implement an information security program that included planning, assessment, and protection. (**Chapter 545**)

Heating, Ventilation, and Air Conditioning (HVAC)
This technology combines three functions into one system. Warmed, cooled, or dehumidified air flows through a series of 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 refers to 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 individual users to 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 SO. (**Chapter 545**)

Information Security Vulnerability Management (ISVM)
The cyclical practice of identifying, classifying, remediating, and mitigating information security vulnerabilities. (**Chapter 545**)

Information System (referred to as "system" throughout this ADS Chapter)
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)
The individual responsible to the senior agency information security officer, the

AO, or information SO for ensuring the appropriate operational security posture for an information system or program is maintained. (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 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, 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 Authorization 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. (**Chapter 545**)

Internet
The collection of interconnected networks that connect computers around the world. (**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, including 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 (e.g., 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 U. S. Department of Defense, the U. S. Department of State, the U.S. Department of Homeland Security, and the U. S. 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 (*i.e.,* mobiles) or on foot (*i.e.,* portables). Such systems are used by emergency first responder organizations, public works organizations, or companies with large vehicle fleets or numerous field staff. The 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 a system. (**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 No. 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 and the benefits of each party will be listed. (**Chapter 545**)

Memorandum of Understanding (MOU)
A document that sets forth a set of intentions between participants. MOUs are generally designed as non-binding instruments and establish political (not legal) commitments. (**Chapters 201, 545, 552**)

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)
The Federal organization responsible for providing records management guidance and for appraising, accessing, preserving, and making available permanent records. (**Chapters 502, 540, 545**)

National Institute of Standards and Technology (NIST)
A non-regulatory Federal agency within the U.S. Department of Commerce. NIST's 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 U. S. 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 (e.g., printers and modems). (**Chapter 545**)

Network Access Control (NAC)
An approach to computer network security that attempts to unify endpoint security technology (e.g., 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 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
Software that can be accessed, used, modified, and shared by anyone. OSS is often distributed under licenses that comply with the definition of "Open Source" provided by the Open Source Initiative (**https://opensource.org/osd**) and/or that meet the definition of "Free Software" provided by the Free Software Foundation (**https://www.gnu.org/philosophy/free-sw.html**). (**Chapter 545, 547**)

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)
Agreement under FAA section 632(b) between USAID and other Federal agencies for specific services or support, where the services or support may be either (1) activity-specific services tied to a specific goal to be performed within a definite time or (2) continuing general professional support services that have a broad objective but no specific readily measurable tasks to be accomplished within a set time. Typically, the other Federal agency would provide the services or support with significant oversight or supervision by USAID (e.g., when Participating Agency personnel provide services in the USAID work space). (**Chapter 306** and **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)
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)
A PIV card is a smart card issued by the Federal Government that contains the necessary data for the cardholder to be granted access to Federal facilities and information systems and assures appropriate levels of security for all applicable Federal applications. A PIV card requires the completion of National Agency background Check with Inquiries (NAC-I) for issuance. (**Chapter 545**)

Personal Identity Verification Alternative (PIV-A)
A PIV-A card is issued to users who are unable to obtain a standard PIV due to restrictions prohibiting issuance to non-U.S. citizens (e.g., USAID Foreign Service Nationals, Third Country Nationals). A PIV-A card requires the

completion of a National Agency background Check (NAC) for issuance. (**Chapter 545**)

Personal Services 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)
Per **OMB A-130**, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available—in any medium and from any source—that, when combined with other available information, could be used to identify an individual. (**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
USAID policy includes both mandatory guidance (i.e., policy directives and required procedures and internal mandatory references), as well as broader official statements of Agency goals, guiding principles, and views on development challenges and best practices in addressing those challenges. (**Chapters 501, 504, 508, 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 Analysis (PTA)
Provides a high-level description of an information system, including the information it contains and how it is used. A 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
In the context of this document, it refers to 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
Senior member of a Development Objective Team or Mission Technical Office who is responsible for the management of an entire program, if not individual projects, activities, and/or awards who may not be the same as the Program Manager designated in the Global Acquisition and Assistance System (GLAAS). (**Chapters 300, 508, 545, 629**)

Program-Specific Policies
These policies define the information security program (i.e., 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. RPO gives system 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 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 Authorization 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)
Refers to DoS, Bureau of Diplomatic Security Special Agents. They are responsible to the Chief of Mission at U.S. posts abroad. An 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 an organizational system by a user, or processes acting on behalf of a user, communicating through an external network (i.e., the Internet). Remote access methods include dial-up, broadband, and wireless. (Source: **NIST SP 800-53, Rev. 5**) (**Chapter 545**)

Remote Desktop Protocol (RDP)
This protocol 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. (**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: **National Security Telecommunications and Information Systems Security Instruction [NSTISSI] No. 1000, National Information Assurance Certification and Accreditation Process [NIACAP]**) (**Chapter 545**)

Risk Executive
An individual or group within the Agency that helps ensure that risk-related considerations for individual information systems, including authorization decisions, are viewed from the perspective of USAID's strategic goals and objectives to carry out its core missions and business functions. (Source: **NSTISSI 1000**) (**Chapter 545**)

Risk Management
The process concerned with the identification, mitigation, and elimination of threats to, and vulnerabilities of, an information system to a level commensurate with the value of the assets protected. (Source: **NSTISSI 1000**) (**Chapter 545**)

Role
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 the 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

the 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, and 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 (i.e., 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. Within a building or facility, SOC is a central location from where staff supervises the site, using data processing technology. Typically, it is equipped for access monitoring and for controlling 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**)

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 (See **The Freedom of Information Act**; **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 during a deliberative process (or a civil discovery process), including attorney-client privilege or a 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 (SLA)
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 offer 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 that uses standardized communications protocols allowing the exchange of short text messages between fixed lines or mobile phone devices. (**Chapter 545**)

Site
"A site is the total computing environment that automated information systems, networks, or components operate. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other information systems." (Source: ***DON DIACAP Handbook*, v1.0, July 15, 2008**) (**Chapter 545**)

Social Media
Applications and/or websites allowing users to engage in social networking. (**Chapters 502, 545, 558**)

Social Security Number (SSN)
A nine-digit number issued by the Social Security Administration to U.S. citizens, permanent residents, and temporary (working) residents under section 205(c)(2) of the Social Security Act, codified as 42 U.S.C. § 405(c)(2). Its primary purpose is to track individuals for social security purposes. (**Chapter 545**)

Special Publication (SP)
A NIST-published document that is 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 can perform higher-order tasks, including technical operations prohibited for other general users. They are 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 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)
Individuals responsible for the 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
System-specific policies apply to single systems and 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
A voluntary work arrangement where an employee performs assigned official duties and other authorized activities during any part of regular paid hours at an approved alternative worksite on a regular and recurring or a situational basis. (**Chapters 405, 508, 531, 545**)

Terms of Service (TOS)
Also known as Terms of Use and Terms & Conditions, TOS refers to rules with which one must agree to abide by to use a service. Sometimes they are used as a disclaimer, especially regarding the use of websites. (**Chapter 545**)

Third-Party
The term refers to any non-Agency staff. (**Chapter 545**)

Third-Party System
An IT system that is external to a system. (**Chapter 545**)

Third-Party Websites
Sites hosted in 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 (*e.g.,* 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, it refers to the block cipher that applies the 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's 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, 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, July 15, 2008) (**Chapter 545**)

Unclassified Information
Information that has not been determined, per **E.O. 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 DHS, US-CERT serves as the focal point for cybersecurity issues in the United States. US-CERT is a partnership between DHS 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. US-CERT also 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 setting

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 information systems and may have no access to USAID 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 virus is a small computer program that has the capability to self-execute and replicate on the infected machine and other machines. Viruses can cause damage to data, make computer(s) crash, display messages, provide back doors, among others. Viruses, as opposed to worms, are meant to replicate themselves on a given system. The term virus is sometimes used to generically describe viruses, but it also can refer to worms and Trojans collectively. (**Chapter 545**)

Visitor
An individual who is not authorized to access the USAID facility but has gained access and 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
Refers to 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 (*e.g.,* spread-spectrum or OFDM radio) and provides 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. It can be used for communication among the personal devices themselves (e.g., intrapersonal communication) or for connecting to a higher level network and the Internet (e.g., an uplink). (**Chapter 545**)

Wireless Wide Area Network (WWAN)
It is 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 a 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_032823