Information Security Requirements for Acquisition of Unclassified Information Technology

A Mandatory Reference for ADS Chapters 302 and 545

Partial Revision Date: 05/31/2024
Responsible Office: M/CIO and M/OAA/P
File Name: 302mah_053124

I. Introduction

Information security, also known as (INFOSEC), is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information in order to provide:

a. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

b. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

c. Availability, which means ensuring timely and reliable access to and use of information.

These are collectively referred to as the "CIA triad." INFOSEC is a general term that can be used regardless of the form the data may take (e.g. electronic, physical). However, the purpose of this Mandatory Reference (MR) is to address USAID INFOSEC requirements for the protection of Agency information in electronic format under USAID contracts. (Policy and procedures regarding INFOSEC requirements for physical security are discussed separately in ADS Chapters **562**, **565** and **302**).

The INFOSEC requirements of this Mandatory Reference (MR) include those that govern system features and operation, as well as those that govern the behavior of contractors in the development and/or maintenance of these systems. This MR is designed to support Acquisition Planners, Contracting Officers (COs), Contracting Officer's Representatives (CORs), designated Information System Security Officers (ISSOs), and other procurement officials and their staff. CORs/COs must contact M/CIO when an acquisition includes any IT equipment, services or system(s) for use by the Agency directly, or use by the contractor on behalf of the Agency under a contract that requires use of the IT equipment/services or system(s).

The appropriate integration of INFOSEC into applicable IT procurements will result in improvements in 1) meeting Agency goals and program objectives; 2) protecting federal assets; and 3) protecting individual rights. This integration is accomplished by incorporating INFOSEC into planning and award.

II. Scope

This MR applies to all contracts, regardless of the source of funding, when the acquired IT equipment, system(s), or services (including cloud services), is to be used by the Agency directly or used by a contractor on behalf of the Agency under a contract that requires use of that IT equipment system(s) or services. (Note: In cases where third parties house or maintain USAID data, Planners and COs must include INFOSEC requirements in the contract in accordance with the requirements in this MR. See **ADS 509** for guidance on IT for Agency Use and Incidental IT.) This MR can also be applied

whenever a requestor, Contracting Officer, or the cognizant designated ISSO believes it would be in the best interest of protecting USAID's information systems.

The terms "contractor" and "contractor personnel," as used in this MR, apply to all non-personal services contractors and subcontractors, including but not limited to commercial entities, non-profit organizations, educational institutions, and individuals. Assistance instruments (grants, including grants under contracts, and cooperative agreements) awarded to non-governmental organizations should not, typically, support the recipient organization having access to USAID information systems or networks (see **ADS 303, Grants and Cooperative Agreements to Non-Governmental Organizations**, and **ADS 304, Selecting the Appropriate Acquisition and Assistance (A&A) Instrument**). If the unique nature of the program USAID is supporting through the grant or cooperative agreement justifies the recipient organization having such access, then the sponsoring office must obtain the approval of the CIO in accordance with the policy and procedures in **ADS 303, Grants and Cooperative Agreements to Non-Governmental Organizations**.

III. Applicable Information System Security Law, Publications, Contract Clauses and Special Requirements

The requirements in this MR were adapted from the guidance in the National Institute for Standards and Technology (NIST) **Special Publication 800-64, Security Considerations in the System Development Lifecycle Rev. 2** and NIST Interagency Report NISTIR 4749, Sample Statements of Work (SOWs) for Federal Computer Security Services. USAID's policies on security for unclassified information system assets are prescribed in **ADS 545, Information Systems Security**, and associated references.

This MR augments the requirements in the Federal Acquisition Regulation (FAR); including Parts 4, 24, and 39, as well as the corresponding policy in the Acquisition Regulation (AIDAR). In addition, **AAPD 16-02 (Revised)** provides special contract requirements to ensure compliance with federal Information Technology (IT) security and accessibility requirements and guidelines, such as Federal Information Security Management Act (FISMA), OMB Circular A-130 Management of Federal Information Resources, and M-14-03 Enhancing the Security of Federal Information and Information Systems. The Office of Management and Budget (OMB) Circular A-130, which implements FISMA, requires agencies to incorporate INFOSEC into their information systems and services acquisition process.

The AIDAR and AAPD 16-02 (Revised) contain requirements for all USAID contractors to comply with USAID policies in safeguarding unclassified information, including Sensitive But Unclassified (SBU), USAID data held, processed, or transmitted via information systems used by USAID or by a contractor on behalf of the Agency. The AAPD addresses USAID requirements for incorporating information system security into awards as specified in **ADS 545**. This MR implements USAID's acquisition-related aspects of federal policies for ensuring the security of unclassified information system

resources.

For additional requirements, questions, and clarification concerning the information in this MR, please contact the Bureau for Management, Office of the Chief Information Officer, Information Assurance Division (M/CIO/IA) at **ato@usaid.gov**. For questions related to the IT security clauses or to request input on a draft SOW, RFP, etc., please contact the M/CIO IT Authorization Team at **ITAuthorization@usaid.gov**. The CIO is the Agency Authorizing Official for all IT systems. Acquisition and Assistance staff may also contact the Bureau for Management, Office of Acquisition and Assistance, Policy Division (M/OAA/P) for questions that are not of an IT technical nature through the M/OAA Policy Mailbox (USAID) at **policymailbox@usaid.gov**.

IV. Roles and Responsibilities

Per **ADS 545**, the following individuals have specific INFOSEC responsibilities in the development and management of contracts for, or that include, the acquisition, operation, and maintenance of USAID information systems, services or networks.

Chief Information Officer (CIO)

The CIO ensures that the INFOSEC requirements of OMB A-130 and other applicable federal regulations and Agency policies are met for all USAID IS acquisition and maintenance contracts.

Chief Information Security Officer (CISO)

The CISO ensures that the security responsibilities under the Federal Information Security Management Act (FISMA) are implemented and maintained during the IT system(s) lifecycle, and serves as a liaison for the CIO to the organization's Information System Owners (SOs), common control providers, and Information System Security Officers (ISSOs). The CISO further ensures that the information system security requirements of OMB A-130 and other applicable federal regulations and Agency policies are met for the acquisition, operation, and maintenance of all USAID information systems, services or networks.

The CISO for USAID must ensure that Information System Security Officers and Contracting Officers incorporate appropriate INFOSEC safeguards into the staffing, design, specification, development, testing, and acceptance of these systems and related IS services. The USAID CISO's INFOSEC duties and responsibilities are further specified in **ADS 545**.

The Information System Owner (SO)

The Information SO is responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The Information SO is responsible for addressing the operational interests of the user

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

Designated Information System Security Officers (ISSO)

Designated ISSOs ensure that the IT systems under their purview maintain operational and maintenance compliance with federal, service provider, and Agency IT security requirements. Designated ISSOs also work with the COR to monitor contractor performance throughout the system life-cycle and ensure that security compliance is established and maintained, and that changes in the system boundary are immediately reported to M/CIO/IA at **ato@usaid.gov**.

Designated ISSOs must coordinate with USAID acquisition officials and M/CIO/IA to determine and ensure that the necessary IT system's security features are adequate and appropriate within the IT contract. Designated ISSOs are responsible for ensuring that adequate security is applied and maintained to IT systems under their purview, throughout the system lifecycle.

Acquisition Planners

Planners must comply with **ADS 300, Agency Acquisition and Assistance (A&A) Planning** and **ADS 509** requirements relating to IT and ensure that:

- INFOSEC requirements are appropriately identified and accurately specified for the CO to include in the contract.

- Adequate funding is available for the total lifecycle costs (including security requirements and decommissioning).

- The acquisition includes M/CIO required INFOSEC specifications appropriate to the system or service's application in the federal and USAID IS operational environment.

- When an IT acquisition includes a cloud-based commercial service, Planners should incorporate Service Level Agreements (SLAs) that provide USAID with continuous awareness of the confidentiality, integrity, and availability of its information; articulate a detailed definition of roles and responsibilities with commercial cloud service providers; establish clear performance metrics with

these providers; and implement remediation plans for non-compliance. SLAs should include:

- The level of performance expected from a cloud service provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified levels are achieved and have been added to contracts with cloud providers, as appropriate;

- Data ownership, licensing, delivery, and disposition instructions specific to the relevant types of government data and government-related data. Disposition instructions should provide for the transition of data in commercially available, or open and non-proprietary format (and for permanent records, in accordance with disposition guidance issued by the National Archives and Record Administration); and

- Appropriate requirements to support applicable inspection, audit, investigation, or other similar authorized activities specific to the relevant types of government data and government-related data, or specific to the type of cloud computing services being acquired.

- The appropriate designated ISSO(s) and/or COR(s) is/are included during the preliminary planning for the system or service and throughout the acquisition process, especially in view of the exponentially escalating technical complexity of security threats associated with new information systems.

Contracting Officer's Representatives (COR)

CORs have a key role in ensuring that cost-effective INFOSEC processes and features are incorporated into Information Systems (IS) products and services as discussed in **ADS 545**. They should understand both the technology associated with the acquisition and the requestor's objectives. They ensure that these factors are integrated in a way that meets USAID's business goals and security requirements, and they oversee contractor performance. CORs must work with the designated ISSO to ensure that the sensitivity assessments for the systems and data associated with the contract are developed and that the appropriate levels of protection are applied to the contract. The information in this MR is designed to assist in achieving these requirements.

CORs who support program acquisitions that are not under the responsibility of a designated ISSO may contact the M/CIO Information Assurance team at **ato@usaid.gov**.

V. Contracts Requiring Security Provisions

INFOSEC must be addressed in all contracts that include Information Technology (IT) resources or services in which a contractor must have physical or logical access to USAID's information contained in unclassified systems that directly support the Agency's mission. This includes IT hardware, software, data, cloud systems and the

services associated with the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Further, cloud systems must meet the security requirements established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) established security baseline: **https://www.fedramp.gov/documents-templates/**. Contracts that contain cloud services should include SLAs that define the level of performance expected from the service provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified levels are achieved (see **Federal Cloud Computing Strategy**).

Examples of contract tasks that require information security provisions include, but are not limited to those that require:

- Access to USAID's Privacy Act-protected data, legally protected data (including source selection information as described in FAR 3.104), financial data, or any commercial data that is proprietary to a third-party entity;

- Acquisition, transmission, or analysis of data owned by USAID; or

- Access to USAID networks or computers at a level beyond that granted to the general public.

VI. Information System Security in the Acquisition Cycle

The application of USAID's INFOSEC policy and security requirements must begin during the concept development of a new system or service and continue through system or service delivery and acceptance (to include issuance of the Authority to Operate (ATO) by the CIO, see **ADS 545**).

A. Planning Phase

The first phase in the acquisition cycle is planning, and it must include INFOSEC considerations.

1) Sensitivity Assessment

During the initial planning phase of the acquisition cycle or task order development, the definition of the security requirement for the product or service being procured begins with a preliminary sensitivity assessment. This sensitivity assessment must be led by the individual who will have the best understanding of the proposed system's technology and technical environment, and its intended application in USAID operations. Usually, this individual will also be designated as the COR for the acquisition. If the need arises at any time during the acquisition cycle, the COR must also initiate a sensitivity assessment.

The sensitivity assessment will be a brief qualitative description of the basic

security needs in terms of integrity, availability, and confidentiality. Legal implications, federal policy, Agency policy, and the functional needs of the system or service determine data sensitivity. Factors including the importance of the system or service to the USAID Mission and the consequences of unauthorized modification, unauthorized disclosure, or unavailability of data must be considered when assessing sensitivity. In this phase, a determination may be made as to whether the system will be treated as a GSS or major application (MA). Such systems normally require additional security considerations such as preparing an information system security plan, including a continuous monitoring plan, incident response and management plan, and naming a designated ISSO for the system.

The sensitivity assessment must include an examination of contract staffing profiles to ensure that there is a clear "separation of duties" throughout the contracted system's development and operational cycles and for any IS services contracted. Separation of duties ensures that no single person has the ability to manipulate the hardware, software, or processing of a system to commit fraud, waste or abuse of USAID systems without the oversight of another person. One example of role conflict could be a contractor's ability to request, award, and pay for a product or service without another person's review and approval. Sensitivity assessments must also consider the concept of "least privilege," where individual contractors or groups of contractors have access only to the systems and data required for their tasks, not "broad" system privileges that may put USAID's information at undue risk.

2) Requirements Analysis

A requirements analysis is an in-depth study of the need for the system or service. The following INFOSEC components must be included in a requirements analysis:

- An analysis of integrity, availability, and confidentiality requirements;
- An updated sensitivity assessment;
- An analysis of the level of assurance required;
- A planning phase risk analysis;
- A preliminary system security assessment and authorization (SA&A) work plan, including project management information, to demonstrate that it complies or will comply with the FISMA and NIST requirements; and
- A Privacy Threshold Analysis (PTA) to determine privacy implications, and if additional privacy compliance documentation is required (Privacy Impact Assessment or System of Records Notice).

This analysis presents a conceptual framework for INFOSEC planning and must include participation by the end users and INFOSEC staff to ensure that operational and security requirements are addressed accurately and in sufficient detail.

3) Other Planning Components

Other parts of the planning process that must incorporate INFOSEC include the following:

- Feasibility study;
- System cost-benefit analysis;
- Software conversion study (if appropriate);
- Analysis of technical alternatives;
- Market surveys conducted by the Planner and CO with M/CIO input; and
- System Inventory and Categorization (FIPS 199) to determine level of security and if an SA&A is required.

Failure to address security comprehensively in the planning cycle and throughout the system's lifecycle could result in acquisition of a system or service without cost-effective security solutions. In instances where M/CIO determines that the security solutions are inadequate for the acquired system or service, the System Owner will be required to address the security deficiencies at their own cost and/or the system will be removed from the USAID network by M/CIO.

B. Solicitation, Award, and Administration

Security requirements must be included in the statement of work (SOW) as specifications, tasks, labor, work, level of effort, etc. SOWs that include cloud services should also include SLAs, as appropriate. Requirements for INFOSEC specifications are contained in guidance from NIST, DHS, OMB, and other federal agencies. Each specification must be justified from the requirements analysis and testable to ensure conformance.

1) Federally Mandated Specifications

Federally mandated or directed INFOSEC specifications are those that are required by law to be included in a solicitation and resulting award. USAID must comply with:

- Federal Information Security Modernization Act of 2014 (FISMA);
- OMB Circular A-130;
- NIST Special Publication 800 Series, and Federal Information Processing Standards (FIPs) requirements; and
- USAID-specific requirements contained in **ADS 545, Information Systems Security**.

Additional detailed guidance and policy directives are provided on the M/CIO **Security Assessment & Authorization (SA&A) Process** site (this content is only accessible from within AIDNet). INFOSEC staff are responsible for assisting Planners and COs in determining whether or not an RFP addresses INFOSEC requirements accurately. If a specification in an RFP will conflict with any federally mandated specification or Agency policy, the Planner/COR must first discuss the specification with the Designated ISSO for coordination of waiver approvals from the appropriate Agency.

Deviations to **ADS 545** policy must be evaluated and cleared by the Bureau for Management, Office of the Chief Information Officer, Information Assurance Division (M/CIO/IA) which is the office responsible for that chapter.

2) Administration

Acceptance must occur only after comprehensive and successful testing of the system's INFOSEC features. Acceptance does not, however, equate to approval to operate ATO. While related to acceptance, ATO is a separate decision based on the risks and advantages of the system and must be granted by the CIO prior to the deployment of the information system. For more information on ATO, see **ADS 545.3.3.12, Security Assessment & Authorization**.

The COR and designated ISSO must monitor contractor performance throughout the system lifecycle to ensure that system security has not degraded over time, and that changes in the environment or system that result in new vulnerabilities are recognized and appropriate safeguards put in place. This is a key role for the designated ISSOs of General Support Systems (GSS) and major applications.

VII. INFOSEC Requirements for Awards

This section discusses general INFOSEC requirements to be incorporated into solicitations and resulting contracts. (See Section C below for recommended language.)

A. All System Developments and Services

1) General INFOSEC Clauses and Special Contract Requirements

a. Designation of ISSO. USAID policy requires that the INFOSEC responsibilities for USAID GSS and major applications be assigned by name to a U.S. citizen employee (either a Direct-Hire in USAID/W or a U.S. citizen employee or USPSC overseas). COs must clearly state the name and location of the designated ISSO in all contracts associated with these systems.

b. Contractor's General INFOSEC Responsibilities. The contract must state the contractor's INFOSEC responsibilities for USAID systems. The CO must include the applicable FAR and AIDAR clauses if all or any part of the contract includes IT resources or services that require the contractor to have physical or logical access to USAID's sensitive information contained in unclassified systems that directly support the Agency's mission. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. References to requirements in other ADS Chapters or federal policy documents (e.g., OMB Circular A-130) may also be added into this Section H language if applicable to the system or service acquisition.

c. Limitation of Use of USAID Information. AAPD 16-02 (Revised) special contract requirement "Restrictions Against Disclosure" emphasizes the contractor's limited ability to use USAID information. However, while effective in limiting the contractor's use of USAID information, the CO, COR, and Designated ISSO must be careful to ensure that all possible contractor information needs are specified in the contract.

2) Contractor Personnel Security

People constitute the most serious threat to USAID's information systems. Their actions, intentional or unintentional, can seriously interrupt or damage USAID's business operations and place personnel and other resources at great risk. The Planner or COR, assisted by the designated ISSO and SEC representative must determine the level of examination and acceptance that will be applied to the contractor personnel who may have access to sensitive data and/or systems under a specific award.

ADS 545, Section 545.3.4.1, Personnel Security, provides the requirements for access to USAID unclassified information systems. At a minimum, any contractor granted access to a USAID system or network must have a facility access determination (formerly known as "Employment Authorization") granted by SEC. More extensive personal examinations or investigations may be required at a level appropriate for the information to be accessed. SEC will assist Planner/CORs in determining the type and level of investigation and authorization required for the security of the various categories of USAID

information.

USAID's most valuable INFOSEC tools are user security awareness, user knowledge of INFOSEC requirements, and user behavior expectations at USAID. Users gain this knowledge initially by taking USAID's new user awareness and training programs, available in bi-weekly classes and on the USAID intranet. All USAID and contractor personnel system users must reinforce their knowledge annually by taking the USAID cybersecurity awareness training course on the intranet. All users are enrolled and notified via USAID University to complete mandatory USAID intranet courses annually.

USAID CORs and designated ISSOs must ensure that contractors employ security precautions of "separation of duties," "need to know," and "least privilege" in all contractor personnel assignments. Separation of duties ensures no single person has the ability to manipulate the hardware, software, or processing of a system to commit fraud, waste or abuse of USAID systems without the oversight of another person. Need to know limits contractors' access to only that information required to perform their roles. Least privilege limits access to only those systems, networks, and files essential for contract performance. Compliance with and knowledge of these tools and concepts is required before any information system access is granted.

The application of these tools and concepts is especially important if contractor personnel will have access to USAID or other government Sensitive but Unclassified (SBU) information that requires an extra measure of protection. COs must include the applicable FAR and AIDAR clauses, and special contract requirements in AAPD 16-02 (Revised) in the solicitation/contract. The contract requirements state the personnel security requirements to ensure that contractors implement these requirements and the expected INFOSEC behavior of their staff while designing, developing, using, and maintaining USAID systems.

3) Contractor Facility Security

USAID contractors using non-USAID facilities and information systems to provide products or services to USAID are expected to provide the degree of security protection commensurate with the sensitivity of the USAID system access and information used for contract performance. CORs, designated ISSOs, and SEC must collaborate to ensure that appropriate contract INFOSEC specifications are provided to the CO for incorporation into the resulting contract in order to protect USAID information resources in the contractor's environment.

B. Hardware, Software, and Services Procurements at USAID/W and Missions

1) System Design and Development

a. IT procurements for the design or development of USAID information

systems, services, networks or major applications require the preparation and maintenance of a Security Assessment & Authorization Plan (SA&A) within 30 calendar days.

b. Additional reference documents may be appended to this language if essential to the system development. However, coordinating and communicating a common "interpretation" of additional references among the government and prospective contractors may not be cost effective.

c. The USAID CISO may also determine that a contractor must prepare an SA&A Plan for other information system developments when this plan is in the best interest of USAID. If this is the case, the USAID CISO will request that the CO responsible for that particular contract take the appropriate action to incorporate this requirement into the contract.

2) System Modifications, Operations, and Maintenance

IT procurements for the modification, operation, and/or maintenance of existing USAID GSS, major applications, or Mission systems must reflect the requirement of adhering to the current INFOSEC Plans for those systems and Missions.

3) System Security Plan Development

For those systems that the contractor has primary operational responsibility on behalf of USAID, the contractor is required to develop and maintain a Systems Security Plan, including a continuous monitoring plan (for both cloud and non-cloud systems) in accordance with the terms of the award. AAPD 16-02 (Revised) special contract requirement "Security Requirements for Unclassified Information Technology Resources", sets forth the requirements which implement **ADS 545** (and its associated references, NIST **SP 800-137** and NIST **SP 800-53, Rev. 4**). The plan must describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under the contract. The plan must also describe those parts of the contract to which it applies. Systems Security Plans must demonstrate a thorough understanding of **ADS 545**, NIST SP **800-137** and NIST SP **800-53 Rev. 4** requirements. Please note: in cases where the IT system is not the property of the government but processes USAID information, an SA&A must be done independent of USAID, to include the selection of a Federal Risk and Authorization Management Program (FedRAMP) approved independent Third Party Assessor (3PAO). See FedRAMP authorized cloud systems at **https://marketplace.fedramp.gov/products.**

Systems Security Plans must include, at a minimum, security measures and program safeguards to ensure that the information system resources developed, acquired, operated, maintained, and/or used by contractor personnel provide the following:

a. Protection from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

b. Continuity of information systems (IS) support for USAID Missions, organizations, programs, and functions;

c. Management, operational, and technical controls sufficient to provide cost-effective assurance of the systems' confidentiality, integrity, and availability;

d. Appropriate technical, personnel, administrative, environmental, and access safeguards;

e. A virus protection program for all IS resources under their control;

f. A network intrusion detection and prevention program for all IS resources under their control; and

g. A continuity of operations plan in the event of a major system failure or disaster.

The CO must obtain the concurrence of the USAID CIO before granting contractor requests for a waiver of any INFOSEC requirements associated with a Systems Security Plan.

Additional information on the development of Systems Security Plans and Continuous Monitoring Plans can be found on the M/CIO IT Services Security Assessment & Authorization Process intranet site: **https://pages.usaid.gov/M/CIO/security-assessment-and-authorization-saa**. The USAID SA&A Web site also provides access to an automated tool to assist in SA&A Plan development. Note: A System Owner (SO) is responsible for ensuring the continuous monitoring of a non-cloud or cloud system. In addition, an SO, in alignment with security programs administered by the USAID Chief Information Security Officer (CISO) and in coordination with the appropriate Information System Security Officer (ISSO), has chief responsibility for system security.

C. Recommended Contract Language

In addition to the required FAR and AIDAR clauses and the special contract requirements found in AAPD 16-02 (Revised), COs must include the following language in the appropriate sections of the solicitation and contract identified below. COs may tailor this language as needed, provided that any variations are not inconsistent with **ADS 545** and **ADS 545** references:

1) Include in Section F - Deliveries or Performance:

CO and Acquisition Planners must ensure that the contract requires that the contractor submit for USAID approval, all plans required for System Assessment and Authorization as outlined in the **USAID Security Assessment & Authorization (SA&A) Process** within 30 days after contract award.

The required plans for SA&A include, but are not limited to the following:

a. Incident Response and Management Plan;

b. Continuous Monitoring Plan;

c. System Security Assessment and Authorization work plan, including project management information (see also AAPD 16-02 [Revised] special contract requirement, Security Requirements for Unclassified Information Technology Resources); and a

d. Configuration Management Plan (see **ADS 545.3.16.9**).

For cloud systems, the contract must also include a requirement for submitting a system security assessment by an accredited Third-Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan (see AAPD 16-02 [Revised] special contract requirement Cloud Computing). Additionally, contracts for cloud systems should include commercial terms and conditions (e.g., license agreements), End User License Agreements (EULAs), Terms of Service (TOS), or other similar legal instruments or agreements. Any applicable service provider terms and conditions should be incorporated into the contract by attachment or other appropriate mechanism.

2) Include in Section H - Special Contract Requirements

H.X Information Security

a. Identification of the Information System Security Officer (ISSO): The designated Information System Security Officer responsible for information system security for this system is _____, located at _____.

b. All contractor personnel must complete the security processes and meet the requirements specified by the USAID Office of Security for the sensitivity or classification level of the information for which they will require access.

302mah_053124