ADS Chapter 508

Privacy Program

Partial Revision Date: 02/16/2023
Responsible Office: M/CIO/IA
File Name: 508_021623

Functional Series 500 – Management Services
ADS 508 – Privacy Program
POC for ADS 508: William Morgan, wmorgan@usaid.gov

Table of Contents

508.1 OVERVIEW

Effective Date: 01/11/2022

This chapter codifies and describes the USAID Privacy Program's organization, functions, policies, and procedures.

Safeguarding personally identifiable information (PII) and preventing its misuse are essential to ensuring that USAID retains the trust of the American public. USAID's responsibilities are outlined in the **Privacy Act of 1974** and the Federal privacy authorities that followed it, including the **E-Government Act of 2002, Section 208 (P.L. 107-347)**, **the Consolidated Appropriations Act of 2005**, the **Federal Information Security Management Act (FISMA)**, and policy and guidance issued by the President and Office of Management and Budget (OMB).

USAID must establish appropriate safeguards to ensure the confidentiality, integrity, and availability of records, and to protect PII against anticipated threats and hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To accomplish that requirement, USAID must incorporate privacy analysis into each stage of the data lifecycle: collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal. These actions are collectively known as processing.

The Privacy Program supports USAID Bureaus, Independent Offices, and Missions (B/IO/Ms) by assisting the Agency in balancing its need to maintain information about individuals while protecting the rights of individuals against unwarranted invasions of their privacy resulting from the processing of their personal information.

The Privacy Program, under the Bureau for Management, Office of the Chief Information Officer (M/CIO), monitors Federal privacy laws and policy through OMB and Federal Privacy Council (FPC) newsletters, emails, and guidance documents for changes that affect the Privacy Program. This information contributes to the program's strategic development of a privacy program plan to identify how the Agency will implement applicable policies, procedures, and privacy controls. The Privacy team reviews the Privacy Program Plan, applicable policies, and standard operating procedures (SOPs) annually and updates them as needed.

This policy applies to all members of the USAID workforce, as well as the processes, and information technology (IT) services, information systems (ISs), and information owned by or operated on behalf of USAID. It is designed to protect Agency PII holdings.

Throughout this chapter, the term "workforce" refers to individuals working for or on behalf of the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems. The term includes U.S. Direct-Hire employees, personal services contractors, fellows, interagency personnel, and contract personnel. Contractors are not normally subject to Agency policy and procedures as discussed in **ADS Chapter 501, The Automated Directives**

System. However, contract personnel are included here by virtue of the applicable clauses in the contract related to HSPD-12 and information security requirements.

For more information on the USAID Privacy Program, see **http://www.usaid.gov/privacy**.

Note: Links to documents other than policies, mandatory references, and documents and websites external to USAID are accessible only to readers with USAID network access.

508.2 PRIMARY RESPONSIBILITIES

Effective Date: 01/11/2022

a. The **USAID Administrator (A/AID)** ensures that Federal privacy requirements are implemented. The Administrator designates the Senior Agency Official for Privacy (SAOP).

b. The **Senior Agency Official for Privacy (SAOP)** has Agency-wide responsibility and accountability for ensuring the Agency's implementation of privacy protections, including USAID's full compliance with Federal laws, regulations, and policies related to privacy.

c. The **Bureau for Management, Office of the Chief Information Officer (M/CIO)** oversees:

- The Agency's information resource management, as defined in the **E-Government Act of 2002** and **OMB Circular A-130, "Managing Information as a Strategic Resource"**;
- The purchasing and supervision of the Agency's IT resources, as defined in **OMB Circular A-130** and the **Federal Information Technology Acquisition Reform Act (FITARA)**; and
- All functions mandated by the **Clinger-Cohen Act of 1996** (see **ADS Chapter 509, Management and Oversight of Agency Information Technology Resources**).

d. The **Chief Privacy Officer (CPO)** is designated by the Bureau for Management, Assistant Administrator (AA/M) to provide oversight and guidance for privacy policy and procedures, compliance activities, and reporting. Consistent with the **Consolidated Appropriations Act of 2005**, the CPO ensures that the Agency-wide Privacy Program is effective, that privacy requirements are incorporated into each stage of the information lifecycle, and that Data Loss Prevention (DLP) processes are developed and implemented to protect Sensitive But Unclassified (SBU), Privacy Act protected information and other PII in electronic and hardcopy data. The CPO also mitigates risks to USAID business operations from privacy data loss.

e. The **Privacy Program's Privacy Team** in the Bureau for Management, Office of the Chief Information Officer, Information Assurance Division (M/CIO/IA) is responsible for day-to-day privacy activities, including compliance documentation, oversight, coordination, guidance, review and approval for Privacy Threshold Analysis (PTAs), Privacy Impact Assessments (PIAs), Privacy Act Statements on Notices on USAID forms, and System of Records Notices (SORNs). The Privacy Team also provides input to all privacy awareness training to employees, privacy incident analysis, and privacy breach response recommendations and coordinates with USAID officials and employees on privacy protection and compliance activities.

f. The **Chief Information Security Officer (CISO)** is designated by the CIO and is responsible for managing the monitoring of USAID systems for privacy breaches and reporting USAID privacy incidents through the USAID Computer Security Incident Response Team (CSIRT). The CISO coordinates with the Bureau for Management, Office of the Chief Information Officer, IT Operations Division (M/CIO/ITO) to implement DLP architecture and/or enterprise configurations.

g. The **Computer Security Incident Response Team (CSIRT)** coordinates and supports the response to computer security events and incidents. CSIRT handles all Agency computer security and classified spillage incidents and works with the Privacy Team to address PII-related incidents. CSIRT is the central reporting authority to the U.S. Computer Emergency Readiness Team (US-CERT). CSIRT analysts investigate, resolve, and report DLP security violations to US-CERT.

h. The **Bureau for Management, Office of the Chief Information Officer, Security Operations Center (SOC)** investigates incidents recorded in the DLP automated tool for false positives and interdicts non-encrypted emails containing PII by placing them in quarantine. SOC ensures that workforce members do not send sensitive or critical information outside the USAID network. The CSIRT team, SOC's specialized response team, addresses incidents using DLP tools.

i. The **Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD)** manages and responds to Agency Freedom of Information Act (FOIA) requests and appeals, pursuant to the law (see **5 U.S.C. § 552**). M/MS/IRD manages and responds to Privacy Act of 1974 access and amendment requests, in addition to maintaining an accounting of Privacy Act disclosures, pursuant to the law (see **ADS Chapter 507, Freedom of Information Act** for more information about FOIA).

Additionally, M/MS/IRD manages USAID's compliance with the **Paperwork Reduction Act (PRA)** and submits completed SORNs on behalf of the Agency to the Federal Register and OMB. M/MS/IRD also submits forms and surveys requiring Privacy Act Section (e)(3) statements for all information collection requests (ICRs).

j. The **Bureau for Legislative and Public Affairs (LPA)** assists with posting privacy policies on all USAID websites, providing alerts to **www.usaid.gov**, explaining that visitors are being directed to a non-government website, and branding and marking USAID's presence on third-party websites.

k. The **Office of the General Counsel (GC)** interprets privacy statutes, regulations, and other legal authorities. GC also reviews reports, SORNs, proposed rules, and other related matters that USAID publishes in the Federal Register, posts on **www.usaid.gov** for legal sufficiency, and submits to Congress, OMB, or other parties.

l. The **Office of the Inspector General (OIG)** monitors the integrity, efficiency, and effectiveness of USAID Privacy Program policies, activities, and reporting. OIG administers FOIA and the Privacy Act with respect to its own records (see **ADS 507** for more information about FOIA).

m. **Heads of Bureaus, Independent Offices, and Missions (B/IO/Ms)** ensure the privacy and confidentiality of the PII their programs and employees collect, use, maintain, and disseminate and for complying with Federal privacy authorities.

n. **Contracting Officers (COs)** ensure that USAID contracts have sufficient privacy clauses to ensure contractor compliance with Federal privacy authorities and protection of the PII under the contract, such as PII processed by USAID or its partners (see **ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology**).

o. **Agency Officials** must consult with the M/CIO Privacy Team to include sufficient privacy safeguards in USAID interagency agreement documents to address data privacy matters including roles and responsibilities for compliance with Federal privacy requirements.

p. **Program Managers (PMs)** are the government officials responsible and accountable for the conduct of a specific government program. PMs ensure the appropriate processing of that program's PII and promote a program's compliance with Federal privacy authorities.

q. **System Owners (SOs)** are organizational officials responsible and accountable for the procurement, development, integration, modification, daily operation and maintenance, and disposal of an information system. The SO ensures adequate resources are allocated for the operation and maintenance of the system, to include Security Assessment and Authorization (SA&A), Plan of Action and Milestones (POA&M) remediation, and other security-related efforts throughout the system's lifecycle.

r. **System of Records Managers** are government officials who are responsible and accountable for the conduct of government programs, ensure the privacy and

security of the PII processed by their Privacy Act system of records, and comply with Federal privacy authorities.

s. Contracting Officer's Representatives (CORs) and **Agreement Officer's Representatives (AORs)** ensure the privacy and security of documents or datasets that contain PII that are created by the contracts or agreements they manage. They also ensure their compliance with Federal privacy authorities (see **ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology**).

t. Information System Security Officers (ISSOs) are responsible for supporting the CISO and information SOs goals for maintaining the appropriate operational security posture for their IT systems or programs. They also ensure the security of the PII processed by their IT systems or programs and their compliance with Federal privacy authorities.

u. USAID Supervisors ensure that the workforce receives instruction and training on safeguarding PII. Supervisors may be subject to disciplinary action for failure to take appropriate action upon discovering a breach or failure to appropriately safeguard PII.

v. The **USAID Workforce** is responsible for complying with the requirements of the Privacy Act and other Federal privacy authorities, which require employees to protect the PII entrusted to their care from unauthorized exposure, complete privacy compliance activities, report PII incidents and breaches, and reduce the volume and types of PII to only what is needed for program functions. Members of the workforce are required to successfully complete cybersecurity and privacy annually and remedial training when assigned.

w. The **Authorizing Official (AO)** is the Agency 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 AO is the CIO.

x. The **USAID Privacy Council** is a subcommittee of the Management Operations Council (MOC). The MOC is comprised of members from B/IOs and chaired by the Agency's CPO. The USAID Privacy Council:

- Supports the SAOP and the CPO to ensure Agency compliance with all applicable privacy-related statutes, Executive Orders, rules and regulations, and policies (see **https://pages.usaid.gov/privacycouncil/about-us**);

- Oversees the Agency's privacy policies and practices and management of privacy risks; and

- Reviews and approves Agency plans and reports regarding mitigation and remediation of privacy-related weaknesses and deficiencies, as well as external reports on Agency compliance with applicable privacy policies and laws.

y. The **Senior Agency Official for Risk Management (SAORM)** is designated by the Administrator and has Agency-wide responsibility and accountability for the implementation of USAID's cybersecurity risk management measures (see **OMB Memorandum 17-25, "Reporting Guidance for Executive Order on Strengthening the CyberSecurity of Federal Networks and Critical Infrastructure"**). These responsibilities include ensuring that cybersecurity risk management processes align with strategic, operational, and budgetary planning processes in accordance with **44 U.S. Code (USC) Chapter 35, Subchapter II: Information Security**. The SAORM works closely with the Agency's Executive Management Council on Risk and Internal Control (EMCRIC). At USAID, the SAORM is the CIO.

z. The **Executive Management Council on Risk and Internal Control (EMCRIC)**, chaired by the Deputy Administrator, is the most senior body charged with reviewing and providing penultimate approval of the Agency's **Federal Managers Financial Integrity Act of 1982 (FMFIA)** assurance statement, risk profile, and proposed corrective measures and risk response and provides oversight for the Agency's Enterprise Risk Management (ERM) practices and internal control systems. The EMCRIC reports to the Administrator, who provides final approval on the EMCRIC's recommendations.

508.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

508.3.1 Personally Identifiable Information

Effective Date: 01/11/2022

It is USAID policy to safeguard individuals' privacy in a manner consistent with the Privacy Act, E-Government Act, OMB directives, and other federal requirements concerning privacy.

Per **OMB A-130**, PII is "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."

Members of the USAID workforce must protect PII from being compromised through inadvertent or purposeful disclosure. PII examples include name, address, social security number (SSN) or other identifying number or code, parent's maiden name, date of birth, place of birth, driver's license number, medical record or medical record number, telephone number, and email address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (*e.g.,* zip code), and other descriptors used to identify specific individuals.

Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. While performing this

assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available—in any medium or from any source—that would make it possible to identify an individual.

To determine whether information is or may become identifiable, USAID evaluates each individual data element that is PII, as well as all of the data elements together.

The sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals' names may depend on the source of the information, the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information. In addition, when determining the privacy and associated risks, the Agency must also consider the volume of PII. A higher volume of PII about a single individual or multiple individuals may pose increased privacy associated risks.

When identifying PII under the Privacy Act, the term "individual" refers to a citizen of the United States or an alien lawfully admitted for permanent residence. USAID uses the Fair Information Practice Principles (FIPPs), as defined in section **508.3.2**, to govern the collection and use of all PII collected by, or on behalf of, the Agency regardless of the individual's nationality. The Privacy Act of 1974 provides additional rights related to access and redress for citizens and permanent residents of the United States.

Section 208 of the E-Government Act uses the term "information in an identifiable form" to mean any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Information in an identifiable form fits within the definition of PII.

The **Privacy Act** uses the term ''record,'' which means any item, collection, or grouping of information about an individual that is maintained by an agency (*e.g.,* education, financial transactions, medical history, and criminal or employment history) and that contains their name or the identifying number, symbol, or other identifying particular assigned to the individual (*e.g.,* a finger or voice print or a photograph).

508.3.2 Privacy Framework

508.3.2.1 Fair Information Practice Principles
Effective Date: 01/11/2022

It is USAID policy to follow the **Fair Information Practice Principles (FIPPs)**, which serve as the foundation of the **Privacy Act**, **Section 208 of the E-Government Act**, and OMB privacy policies applicable to all Federal agency information systems and organizations. FIPPs frame the privacy risks and mitigation strategies required to protect and ensure the proper handling of PII. The USAID Privacy Program uses the

following FIPPs as a framework for organizing and addressing privacy protections when considering privacy in USAID programs throughout the information lifecycle.

a. Authority and Purpose. Articulate the specific authority that permits the collection of PII and the purposes and intent of PII use.

b. Accountability, Audit, and Risk Management. Provide accountability for compliance with all applicable privacy protection requirements, including all identified authorities and established policies and procedures that govern the collection, use, maintenance, and dissemination of PII; and audit for the actual use of PII to demonstrate compliance with established privacy controls.

c. Data Quality and Integrity. Ensure, to the greatest extent possible, that PII use is accurate, relevant, timely, and complete, as identified in the public notice (see section **508.3.4.5** for more information on the public notice requirement).

d. Data Minimization and Retention. Collect only PII that is directly relevant and necessary to accomplish the specified purposes. Only retain PII for as long as necessary to fulfill the specified purposes and in accordance with the appropriate National Archives and Records Administration (NARA)-approved record retention schedule and **ADS Chapter 502, The USAID Records Management Program**.

e. Individual Participation and Redress. Involve the individual in the decision-making process regarding the collection and use of their PII, seek individual consent for the collection, use, maintenance, and dissemination of PII, and provide a mechanism for appropriate access to and amendment of the PII.

f. Security. Protect PII (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

g. Transparency. Provide notice to the individual regarding the collection, use, maintenance, and dissemination of PII.

h. Use Limitation. Use PII solely for the purposes specified in the public notice and share information compatible with PII intent and objectives.

508.3.2.2 NIST Privacy Framework

Effective Date: 01/11/2022

The **NIST Privacy Framework** provides guidance on "finding ways to continue to derive benefits from data processing while simultaneously protecting individuals' privacy." The Privacy Framework's purpose is to help organizations manage privacy risks by:

- Taking privacy into account as they design and deploy systems, products, and services that affect individuals;
- Communicating their privacy practices; and
- Encouraging cross-organizational workforce collaboration, for example, among executives, legal, and IT through the development of profiles, selection of tiers, and achievement of outcomes.

508.3.2.3 Privacy Controls

Effective Date: 01/11/2022

The USAID Privacy Program uses PIAs to evaluate the privacy risk associated with Agency systems. USAID privacy controls are based on FIPPs, **Section 208 of the E-Government Act**, the **Privacy Act**, and guidance in **NIST SP 800-53, Rev. 5**.

NIST SP 800-53, Rev. 5, Privacy Controls provide a comprehensive framework for privacy policy and implementation. They establish a structured set of privacy controls based on best practices that will help USAID and the Privacy Program comply with Federal privacy authorities. The publication also establishes a relationship between privacy and security controls for the purposes of enforcing privacy and security requirements within the NIST Risk Management Framework (RMF) and the Privacy Framework. Privacy and security controls are addressed specifically in **ADS 545**.

508.3.2.4 Risk Management Framework

Effective Date: 01/11/2022

The **USAID Information Technology (IT) Systems Accreditation Risk Management Framework (RMF) Handbook** enables management officials (*i.e.,* AO and SAOP) to identify security and privacy risks associated with a system and to use security and privacy controls to reduce the risk to an acceptable level. USAID's RMF Handbook draws on **NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy**, which implements continuous monitoring processes; provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems and business functions; and integrates information security and privacy into the enterprise architecture and System Development Lifecycle (SDLC).

508.3.2.5 System Owner Responsibilities

Effective Date: 01/11/2022

a. Ensures any necessary privacy documentation is drafted and submitted to the Privacy Team for review and approval, the documentation remains accurate and up-to-date and privacy controls and continuous monitoring of the controls are implemented for the IT system per **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations**.

b. Prepares and implements a security plan and monitors its effectiveness (see **ADS Chapter 545, Information Systems Security**).

c. Protects the privacy and security of PII processed by an information system and ensures the system complies with Federal privacy authorities.

d. Incorporates privacy safeguards into the USAID SDLC (**see landing page showing Agile and Waterfall frameworks under SDLC**) to include all mandatory privacy risk and compliance documentation.

e. Must be a U.S. Direct-Hire (see **ADS 545**).

f. Is responsible for rulemaking when Privacy Act exemptions are relevant to the system. The SO can consult with the Privacy Program for guidance on updating Federal Register notices.

508.3.3 Privacy Rules of Behavior (ROB)

508.3.3.1 Workforce Use of USAID Information Systems (No Expectation of Privacy)

Effective Date: 01/11/2022

USAID alerts users of the USAID network and systems with a security/monitoring statement that states that (1) the user is accessing a U.S. Government information system; (2) unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties; and that (3) by entering the system, the user consents to the following:

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

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

- Consent is final and irrevocable. Users may not rely on any statements or informal policies purporting to provide them with any expectation of privacy

regarding communications on this system, whether oral or written, by their supervisor or any other official, except the USAID CIO.

Refer to **ADS 545** for more information on the Agency's Security/Monitoring Statement.

508.3.3.2 Electronic Records Requests (No Expectation of Privacy)

Effective Date: 02/16/2023

Members of the USAID workforce using Government communications resources must understand that such use is generally not secure, is not private, and is not anonymous.

System Managers (SMs) employ monitoring tools to detect improper use as defined in this chapter. Any electronic communications may be disclosed within the Agency to officials who have a need to know in the performance of their duties; for instance, when the CISO, Office of Security (SEC), or GC needs to gain access to an employee's email accounts or phone calls and records for the investigation of a case. Further,

1. Per the authorities contained within the Inspectors General (IG) Act of 1978, the Office of the Inspector General (OIG) may request in writing from the CISO electronic records in the course of investigative matters.

2. The Director of SEC has delegated authority from the Director of National Intelligence (Security Executive) and the Office of Personnel Management (Suitability Executive) to conduct a range of investigations of direct-hire and contract employees related to personnel actions, physical or logical facilities access, counterintelligence issues and concerns as well as the insider threat program. Specific authorities related to these activities are referenced in ADS 101. In the performance of these duties, the Director of SEC may request in writing from the CISO electronic records in the course of investigative matters.

3. The Assistant General Counsel for Ethics and Administration (GC/EA) is tasked with assuring that Agency administrative inquiries are conducted consistently and appropriately. Therefore, all personnel related administrative inquiries, under any authority, must be coordinated with and cleared by GC/EA. To the extent that forensic searches by CISO are deemed necessary pursuant to any administrative inquiry, the specific parameters of such a search must be cleared in advance by GC/EA. Forensic searches in relation to an administrative inquiry must be based on a specific need, must be tailored to the circumstances of the allegation, and must be conducted with the minimum intrusion. Under no circumstances may a forensic search be authorized to locate communications that are protected under the Whistleblower Protection Act or any other protected activity.

4. The Assistant General Counsel for Litigation and Enforcement may request in writing from the CISO electronic records in order to carry out the office's functions.

See ADS 545mam and ADS 545mbd for additional guidance.

508.3.3.3 Privacy Specific Guidance for Complying with Rules of Behavior for Users

Effective Date: 07/06/2022

All members of the USAID workforce must protect PII in any format (*e.g.,* paper, electronic, mobile media, etc.) from unauthorized disclosure. Members of the workforce must:

a. Reduce the volume and types of PII they collect for program functions to the minimum necessary.

b. Have a justifiable business purpose for processing the PII.

c. To protect PII, members of the workforce:

1. Must protect any PII processed through proper collection, storage, transportation, transmission, and disposal methods;

2. Must not access PII beyond what they need to complete their job duties; and

3. Must not disclose PII to unauthorized parties. This includes verbal discussions or processing within earshot of persons without a need to know.

PII is a type of SBU information. As a result, PII requires greater controls against unauthorized access and disclosure than information that is Unclassified. Members of the workforce must:

i. Label documents containing PII with the SBU header and footer and use the green **AID 568-3, SBU Coversheet** with paper documents; and

ii. Protect PII, as well as other SBU information, against unauthorized access or disclosure by ensuring that only those people who have a clearly demonstrated need to know or use the information have access.

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"**).

Failure to protect PII may result in administrative action and criminal and/or civil penalties. Members of the workforce must understand their specific responsibilities to

protect the PII entrusted to them. Protecting PII in USAID's possession and preventing its breach are necessary to ensure USAID retains the trust of the American public.

For more information about workforce responsibilities regarding USAID PII, see **ADS 545mbd, Rules of Behavior for Users**. Misuse, whether intentional or unintentional, or failure to comply with ADS 545mbd may result in disciplinary or adverse actions, in accordance with **ADS Chapter 485, Disciplinary Action - Foreign Service** and **ADS Chapter 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct - Civil Service**.

All members of the workforce must immediately and without delay report all potential, suspected, 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 manner in which the incidents might have occurred. (Note: Users with a usaid.gov email may report suspected or actual privacy breaches or incidents via **servicecentral.usaid.gov** instead of emailing **cio-helpdesk@usaid.gov**.)

For questions about the privacy protection responsibilities of employees, please contact the Privacy Program at **privacy@usaid.gov**. For guidance on policies and procedures for recording audio or video meetings see **ADS 502mah, Policies and Procedures for Recording Audio and Video Meetings**. For information on employee responsibilities for classified information, see **ADS Chapter 552, Cyber Security for National Security Information (NSI) Systems**, and **ADS Chapter 561, Security Responsibilities**.

508.3.3.4 IT Rules of Behavior for Managers

Effective Date: 01/11/2022

This section addresses USAID's policy requirements for the behavior of Agency program managers, System of Records Managers, SOs, ISSOs, and supervisors (managers) under the **Privacy Act**, **Section 208 of the E-Government Act**, and other privacy authorities.

All USAID managers must consider the information lifecycle in evaluating how information handling practices at each stage may affect the privacy rights of individuals. **Section 208 of the E-Government Act** requires that all Federal agencies conduct a PIA for all new or substantially changed technology that processes PII or for a new aggregation of information that is collected, maintained, or disseminated using information technology. For this purpose, program managers responsible for IT systems should complete a PTA at the early program or system design phase for all new or substantially changed technology. For all information systems that are known to process, or will process PII, the SO will be required to complete a PIA and any additional privacy compliance documentation as early in the SDLC as possible. To be comprehensive and meaningful, PTAs, PIAs, and other privacy compliance documentation require collaboration by Privacy Program experts as well as experts in the areas of IT, IT security, records management, and legal counsel, as necessary.

For USAID Privacy Act Systems of Records, Systems of Records Managers must comply with specific responsibilities under the Privacy Act, including making reasonable efforts to maintain accurate, relevant, timely, and complete records about individuals and maintaining only PII considered relevant and necessary for the legally valid purpose for which it is collected.

For USAID information systems containing PII, SOs must incorporate privacy compliance requirements into the SA&A process. This process is an evaluation of an IT system's security and privacy risk(s) and mitigating controls. The SA&A process considers specific security requirements, verifies the existence of security controls, and summarizes residual risk. With the adoption and incorporation of the privacy controls in **NIST SP 800-53, Rev. 5**, SOs must ensure that privacy compliance is part of the system development lifecycle. For more information on the SA&A process, see **NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans** and the **IT Systems Accreditation RMF Handbook**.

A system's ISSO must ensure all relevant security and privacy controls are applied to their system and must audit and/or monitor the system security and privacy controls to ensure the safeguards effectively reduce privacy risks.

USAID supervisors are responsible for ensuring members of the workforce receive instruction and training on safeguarding PII. Supervisors are responsible for educating their staff on safeguarding PII and for taking appropriate steps to address violations of Agency privacy policies, which may include disciplinary action.

508.3.4 USAID Privacy Compliance Documents and Practices

508.3.4.1 Incorporating Privacy into the Data Lifecycle

Effective Date: 01/11/2022

As information and devices become increasingly mobile, the amount of PII collected increases. The proliferation of PII processing expands USAID's privacy footprint and may lead to elevated risks and threats to the Agency. These factors make it more important than ever to consider privacy protections throughout the entire lifecycle of existing and emerging technologies as part of USAID's overall organizational risk management strategy.

OMB directs all Federal agencies to incorporate privacy analysis into each stage of the data lifecycle (*i.e.,* collection, use, retention, processing, disclosure, and destruction), from the early design stage to start up, use, and disposal. The Privacy Program strives to implement substantive privacy protections, such as notice and consent, limitations on data collection and retention, data accuracy, and procedural safeguards aimed at integrating FIPPs into USAID's everyday business operations.

Achieving adequate privacy protections for USAID, its business processes, and its information systems requires planning that incorporates privacy controls in data lifecycle management, especially at the critical initiation phase. In that light, USAID incorporates required privacy compliance documents into its SA&A process, as briefly discussed in section **508.3.3.3**.

508.3.4.2 Privacy Threshold Analysis

Effective Date: 01/11/2022

This section addresses USAID's policy requirements for the creation and maintenance of PTAs. The Privacy Program uses a PTA to (1) determine whether a particular program or information system will introduce privacy risks as it performs its functions; and (2) identify whether the program needs to comply with any privacy protection requirements pursuant to Federal privacy statutes, regulations, and other authorities. The PTA is used to identify if systems process PII and must meet further privacy requirements.

Program managers responsible for IT systems should complete a PTA in the early program or system design phase for any new or substantially changed technology. If no additional privacy concerns are identified by the Privacy Program, the approved PTA will serve as the system's privacy documentation. The PTA/PIA template contains guidance on how to complete a PTA. If a program or system will process more than business contact information or if a new privacy risk to the Agency is indicated, then a PIA is required.

All information systems undergo continuous privacy monitoring. Annually, assigned system points of contact (POCs) (*i.e.,* SO, ISSO, privacy analyst, etc.) will review all corresponding privacy documentation to determine if any privacy-related changes were made to the system. If so, the SAOP must review and approve changes and all stakeholders must re-sign and date privacy documentation. Contact the Privacy Program for the full process details via **privacy@usaid.gov**.

508.3.4.3 Privacy Impact Assessment

Effective Date: 01/11/2022

This section addresses USAID's policy requirements for the creation and maintenance of PIAs as mandated by **Section 208 of the E-Government Act of 2002** and OMB implementing guidance. For all information systems that are known to process or will process PII, the SO must complete a PIA and any additional privacy compliance documentation as early in the SDLC as possible. The PIA is a vital tool used to evaluate possible privacy risks and the mitigation of those risks throughout the development lifecycle of a program or system. The Privacy Program uses the PIA to (1) determine the risks and effects of processing PII; (2) evaluate protections and alternatives to processing PII to mitigate potential privacy risks; (3) address privacy throughout the lifecycle of each system; and (4) ensure compliance with Federal document authorities and USAID policies, procedures, and standards, including providing information to the American public to assure their government properly protects their PII.

USAID must conduct a PIA when:

a. Developing or procuring any new technologies or systems that handle or collect PII including, but not limited to, cloud services, help desk services, professional services, websites, tools, mobile applications, and databases;

b. Creating a new program, system, technology, or information collection that may have privacy implications;

c. Updating a system that results in new privacy risks; and

d. Issuing rulemaking that involves the collection of PII.

See **ADS Chapter 300, Agency Acquisition & Assistance (A&A) Planning** and **ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology** for guidance on IT acquisitions.

The SO (or other stakeholders) must draft or update PIAs when significant changes are made to an information system. Significant changes include:

- Conversions: When converting from paper-based records to electronic systems;
- Anonymous to Non-Anonymous: When functions applied to an existing information collection change anonymous information into information in an identifiable form;
- Significant System Management Changes: When new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- Significant Merging: When agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, and matched with other databases or are otherwise significantly manipulated;
- New Public Access: When user-authenticating technology (*e.g.,* password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- Commercial Sources: When agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources;

- New Interagency Uses: When agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

- Internal Flow or Collection: When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form; or

- Alteration in Character of Data: When new information in identifiable form added to a collection raises the risks to personal privacy (*e.g.,* the addition of health or financial information).

All information systems undergo privacy continuous monitoring. Annually, assigned system POCs (*i.e.,* SO, ISSO, privacy analyst, etc.) will review all corresponding privacy documentation to determine if any privacy-related changes were made to the system. If so, the updates must be reflected in the PIA and all other privacy compliance documentation. The SAOP, CPO, and/or their designee(s), must review and approve significant changes.

508.3.4.4 Third-Party Website PIA

Effective Date: 01/11/2022

In addition, pursuant to the guidelines in **OMB M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications,"** USAID must conduct a PIA when the Agency or one of its contractors on the Agency's behalf uses a third-party website or application to engage with the public. In general, a USAID program should conduct a single, separate PIA for each third-party website or application. For more information on third-party websites, refer to the Project Website Approval Procedures at: **https://pages.usaid.gov/LPA/Website-governance-board-approval-procedures** (Note: This link is only accessible to USAID.gov users).

B/IO/Ms must take specific steps to protect individual privacy whenever they use third-party websites and applications to engage with the public. USAID SOs must comply with this policy, in conjunction with the Privacy Act and all applicable laws, when implementing third-party website and application services. The responsible SO must adhere to the following requirements:

a. Third-Party Privacy Policies. SOs must examine the third party's privacy policy to evaluate the risks and determine whether the website or application is appropriate for the Agency's use and continue to monitor that appropriateness.

b. External Links. SOs must ensure that an alert is provided to third-party website/application visitors explaining that they are being directed to a non-government website that may have different privacy policies from those of the Agency's official website.

c. Embedded Applications. SOs must take the necessary steps to disclose the third party's involvement when the website/application is embedded in the USAID website.

d. Agency Branding. SOs must apply appropriate branding to distinguish USAID activities from those of non-government actors (see **USAID Graphic Standards Manual and Partner Co-Branding Guide** for more information).

e. Information Collection. SOs must ensure that USAID collects only the minimum PII necessary to accomplish a purpose required by statute, regulation, or Executive Order.

f. Third-Party Website PIAs. SOs must conduct a third-party website PIA whenever USAID's use of a third-party web site or application makes PII available to the Agency.

g. Agency Privacy Policies. SOs must ensure that the USAID website privacy policy accurately describes their use of third-party websites and applications.

h. Agency Privacy Notices. To the extent feasible, the SO must post a Privacy Notice on the third-party website or application itself.

508.3.4.5 Privacy Act Compliance

Effective Date: 01/11/2022

USAID must provide public notice of its information practices and the privacy impact of its programs and activities. USAID accomplishes this function by posting Privacy Act Statements or notices on USAID websites and paper forms and surveys, as well as posting website privacy policies, **PIA summaries**, and SORNs on USAID public websites.

a. Privacy Act Section (e)(3) Statements

All forms, paper and electronic, collecting information under the Privacy Act for a system of records must include a Privacy Act (e)(3) Statement on the form used to collect the information or on a separate form that can be retained by the individual. Additionally, a form's corresponding Privacy Act Statement must be read to, and acknowledged by, the individual prior to them providing information verbally, if the information is collected via phone or in an interview style collection.

Per **Privacy Act, Section (e)(3)**, USAID must provide notice to individuals about whom it collects PII regarding (1) the authority that authorizes the PII collection and whether disclosure by the individual of such PII is mandatory or voluntary; (2) the principal purposes for which the PII will be used; (3) the routine uses that may be made of PII; and (4) the effects on the individual of not providing all or any part of the requested information.

USAID can only make an information collection mandatory when a Federal statute, Executive Order, regulation, or other lawful order specifically imposes a duty on the individual to provide the information, and the individual is subject to a penalty for failing to provide the requested information. In the absence of a lawful order, all disclosures are voluntary, and USAID must make the individual aware of the consequences, if any, of not providing the information; for example, a denial of a privilege or benefit sought by the individual.

The statement must be located and accessible on the form or survey where the PII is collected, whether on a website, electronic media, or paper. A Privacy Act Statement must be included on all USAID forms and surveys (*i.e.,* internal and external) that collect PII on individuals (*i.e.,* citizens of the United States or aliens lawfully admitted for permanent residence).

The Privacy Act Statement Template contains guidance on how to draft a Privacy Act Section (e)(3) Statement or notice. For more information about a Privacy Act Statement or notice, see the **ADS 508mag, USAID Privacy Act Section (e)(3) Statement or Notice Template**.

b. Privacy Act Disclosure Limitations and Routine Uses

The Privacy Act prohibits the disclosure of any PII to anyone except the subject individual absent the written consent of the subject individual or unless the disclosure falls within one of twelve statutory conditions in the **Privacy Act, 5 USC 552a(b)(1)-(12)**. Frequently used disclosure conditions include:

1. To employees who have a need to know in the performance of their duties;

2. Per a FOIA request (for more information about FOIA requests, see **ADS 507**); and

3. Under a routine use specified in the appropriate SORN. For the routine uses specified in SORNs, as required by **OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,"** USAID must ensure that all routine uses remain appropriate and that the recipient's use of the records continues to be compatible with the purpose for which the information was collected.

c. Privacy Act Disclosure Exemptions

The Privacy Act exempts directly and authorizes USAID to exempt certain PII from disclosure, including:

1. Information compiled in reasonable anticipation of a civil action or proceeding (see **5 USC 552a(d)(5)**);

2. Special exemptions for agencies or offices with principal activity pertaining to enforcement of criminal laws (see **5 USC 552a(j)**); and

3. General exemptions (see **5 USC 552a(k)**).

   USAID has exempted certain systems of records under both the Privacy Act special exemptions and general exemptions. (For more information about USAID Privacy Act Exemptions, see **22 CFR 215.13, General Exemptions** and **22 CFR 215.14, Specific Exemptions**). As required by **OMB Circular A-108**, the Agency must review each system of records for which an exemption has been promulgated every four years to determine whether such exemption is still needed.

   Agencies must also submit a draft rule to OMB along with the new or revised SORN(s) associated with the systems that the agency wishes to exempt. SMs are responsible for rulemaking when Privacy Act exemptions are relevant to the system. The SM can consult with the Privacy Team for guidance on updating Federal Register notices. For more information on Agency Rulemaking, see **ADS Chapter 156**.

d. Privacy Act Civil Remedies and Criminal Penalties for Unlawful Disclosure

Violation of the Privacy Act disclosure restrictions carries penalties for those who knowingly violate the law. For information on specific civil remedies and criminal penalties, see the USAID Regulations for Implementation of the Privacy Act of 1974 at **22 CFR 215.12**.

e. Privacy Act System of Records Notices

USAID must conform to the notice requirements of the **Privacy Act**, which also includes SORN requirements. **OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,"** provides more information for review.

The Privacy Act applies to "systems of records," which are a group of records under the control of USAID from which information is retrieved by the name of the individual or by some identifying number, symbol, or other unique identifier assigned to the individual. An "individual" includes a citizen of the United States or an alien lawfully admitted for permanent residence.

When USAID establishes a new system of records or modifies or rescinds an existing system of records, USAID must create and publish a notice of the existence and character of the system of records in the Federal Register. System Owners must complete a draft of the SORN and ancillary documentation using the Privacy Program's templates. A new SORN must be published and be

considered final during the Federal Register process before collecting PII. System Owners must implement continuous monitoring procedures to document changes to the system of records. Such procedures must include requirements for documenting whether changes are significant (as defined in section **508.3.4.3**) and provide a rationale for determining that a change is not significant. Significant changes trigger a requirement to publish a Modified System of Records Notice.

SORNs also indicate whether any records are exempt from certain Privacy Act requirements. Only certain types of records, described in subsections (j) and (k) of the Privacy Act, can be exempted. Exemptions require rulemaking and are not effective until published in a Final Rule. For more information about systems of records and exemptions, see **OMB Circular A-108**.

The SORN Standard Operating Procedure contains guidance on how to complete the SORN and information on the USAID SORN process requirements. The Privacy Program uses the information provided to complete the OMB authorization process, notify the required House and Senate Committees, publish the SORN in the Federal Register, and post it on **www.usaid.gov**. For more information about SORNs, see the **Privacy Forms and Templates page** and **OMB Circular A-108** which provides more information on SORNs.

f. Privacy Act Requests

The **Privacy Act** provides individuals with a means to seek access to and amendment of their records. The **Privacy Act** pertains only to records about individuals who are either U.S. citizens or lawfully admitted permanent resident aliens.

A Privacy Act Request allows U.S. persons to (1) gain access to records retrieved by their name or other unique identifier (unless exempted by a Rule published in the Federal Register, from disclosure) maintained by USAID; (2) seek correction or amendment of inaccurate, irrelevant, incomplete, or outdated information the Agency maintains about them; and (3) to file a suit against the Federal Agency to access or amend its records, or for violations of the Privacy Act.

M/MS/IRD is responsible for managing and responding to Privacy Act access and amendment requests. M/MS/IRD is also responsible for managing correction dissemination and disclosure accounting functions, per the **Privacy Act** and **22 CFR 215, Regulations for Implementation of Privacy Act of 1974**.

508.3.4.6 Freedom of Information Act

Effective Date: 01/11/2022

FOIA provides that any person, regardless of citizenship or immigration status, has a right, enforceable in court, to obtain access to Federal agency records, except such

records (or portions of them) that FOIA exempts from public disclosure. FOIA covers virtually all agency records under the possession and control of a Federal executive branch agency. If an individual is requesting records about themselves held under their name or other individual identifier, that individual can request them under **FOIA**. U.S. persons may request them under both FOIA and the **Privacy Act**.

FOIA exemptions provide protection for nine categories of records, including records for which disclosure would constitute a clearly unwarranted invasion of personal privacy. For more information on FOIA issues and requests, see **USAID FOIA requests** and **ADS 507, Freedom of Information Act (FOIA)**.

508.3.4.7 Information Collections

Effective Date: 01/11/2022

This section addresses the policy requirements applicable to all Agency actions that will result in the collection of information from the public, and/or the collection of personal or identifiable information from USAID workforce members. B/IOs may not collect or sponsor the collection of information from workforce members or the public without prior approval. B/IOs must submit all forms surveys, and questionnaires to **privacy@usaid.gov**, **forms@usaid.gov**, and **508compliance@usaid.gov** for clearance.

The **Paperwork Reduction Act (PRA)** and subsequent regulatory guidance established requirements for ICRs and for minimizing the paperwork burden for individuals, small businesses, educational purposes, non-profit institutions, Federal contractors, state, local, and tribal governments, and other persons from the collection of information by or for the Federal Government. ICRs are a specific type of forms review conducted by OMB. Surveys, questionnaires, registration forms, websites, and databases are subject to PRA requirements.

Information collections are subject to all Federal privacy compliance requirements, including PTAs, PIAs, Privacy Act Statements, and SORNs before a USAID program starts to collect information and again before they make any changes to the program's information collection process. Program managers, System of Records Managers, SOs, and ISSOs, or any ICR stakeholder, must complete these privacy compliance documents, as necessary. For more information, see sections on PTAs, PIAs, SORNs, and Privacy Act Statements in this chapter.

M/MS/IRD is responsible for managing the ICR approval process. Program Managers and SOs must work with M/MS/IRD to comply with the OMB procedures for ICRs. For more information on the ICR approval process, see **ADS Chapter 505, Forms Management Program**, **ADS Chapter 156, Agency Rulemaking**, and **ADS Chapter 506, Reports Management**.

508.3.4.8 Website Privacy Policies

Effective Date: 01/11/2022

SOs ensure that USAID-funded or produced public-facing websites comply with privacy requirements, including posting privacy policies that clearly and concisely inform visitors to the website what information USAID collects about individuals, why the Agency collects the information, and how the Agency will use the information. SOs must provide website privacy policies that are clearly labeled and easily accessed by website visitors and post privacy policies at major entry points and where substantial PII is collected. For more information on website privacy notices, see OMB Memoranda **M 99-18** and **M 10-23**.

SOs must monitor their public-facing websites to ensure compliance with privacy requirements. The CPO may require corrective actions for sites determined to be non-compliant and may shut down sites until the SOs correct the deficiencies. See **ADS 508mak, USAID Public Website Privacy Policies Requirements** and **ADS 557, Website Management and Public Information** for more information about SOs' responsibilities regarding USAID website compliance requirements.

508.3.4.9 Privacy Considerations for Contracts and Information Sharing Agreements

Effective Date: 01/11/2022

Pursuant to **Privacy Act of 1974, Section(m)(1),** Operating Units (OUs) must advise COs when supplies/services under a procurement request involve access to USAID's Privacy Act-protected data, or more specifically, the operation by or on behalf of the Agency of a system of records to accomplish an Agency function. Together, the OU, System of Records Managers, and SOs must coordinate with the COs to make certain contracts include appropriate terms and conditions ensuring contractor compliance with the Privacy Act and **Section 208 of the E-Government Act**.

Requirements set forth in the Federal Acquisition Regulation (FAR), including Part 24, Protection of Privacy and Freedom of Information (privacy training) and Part 39, Acquisition of Information Technology, Agency-specific requirements for privacy under contracts is provided in **Acquisition and Assistance Policy Directive (AAPD) 16-02, Revision 2** and may be found at the **Acquisition & Assistance Policy Directives (AAPDS) and Contract Information Bulletins (CIBS) Webpage** and **ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology**. The **AAPD 16-02, Revision 2** and **ADS 302mah** provide requirements for information technology security and privacy considerations for systems where systems of records are involved.

When **FAR 52.224-3, Privacy Training** is included in the contract as prescribed, contractors are responsible for ensuring all required privacy training (onboarding and annual) is completed by contractor employees. M/CIO/IA provides initial privacy training at the New Entrant Orientation (NEO), and during Annual Privacy Training thereafter, to the entirety of the badged USAID workforce, including contractor and subcontractor employees, for the duration of all USAID contracts through USAID University. The FAR states that a contractor employee must not have access to a system of records or handle PII until the employee completes training.

CORs are responsible for ensuring contractor employees participate in mandatory on-boarding training which is required to obtain access to USAID facilities and IT systems. CORs are also responsible for ensuring that individual contractor employees are aware that they need to set up an account with USAID University and complete the mandatory USAID privacy training annually (see section **508.3.5.2**). See **https://pages.usaid.gov/HCTM/usaid-university** for more information on USAID University. Workforce members who need an account must contact USAID University to request an account via email at **hr-helpdesk@usaid.gov**.

In addition, all COs should consult with their General Counsel to ensure required FAR and USAID IT privacy and security contract clauses are incorporated into solicitation and resulting award, as appropriate.

For more information on IT resources contracting and contracting generally, see **ADS Chapter 302, USAID Direct Contracting**, **ADS 302mah**, **ADS Chapter 331, USAID Worldwide Purchase Card Program**, and **ADS 509**.

a. Privacy Considerations for Data and Information Sharing Agreements

Agency Officials must work with Program Managers, System of Records Managers, and SOs to include appropriate privacy protection language in data and information sharing agreements to ensure compliance with the Privacy Act and the Federal authorities that flow from it, including the **E-Government Act Section 208** and USAID privacy policies.

The agreement should identify the Agency Official responsible for overseeing implementation of the agreement, as well as points of contact for the agreement. The Agency Official must provide overall liaison and coordination for agreements that the Agency Official signs. For more information about Agreement Officers, see **ADS Chapter 103, Delegations of Authority**.

Agency Officials must work with General Counsel, Regional Legal Officers (RLOs), PMs, the M/CIO Data Services Team, the M/CIO Information Assurance Division, System of Records Managers, and SOs to incorporate the following privacy protections in data and information sharing agreements that involve PII:

1. Specific PII elements shared under the agreement,

2. Secure Method(s) for transferring PII,

3. Secure Method(s) for storing PII,

4. Specify roles/individuals authorized to access PII,

5. Specify approved parameters for processing PII,

6. Specify procedures for destroying/deleting/returning PII,

7. Specify protocols to review the effectiveness of the information sharing agreement, and

8. A description of the responsibilities of the parties to the agreement for PII incidents and breach response and reporting activities.

b. Privacy Considerations for Cloud Computing Services

Cloud computing is Internet-based computing whereby USAID contracts for shared resources, software, and information for computers and other devices. While this provides a flexible solution for complex information technology needs, cloud computing poses additional privacy challenges for contract services.

Cloud services must not be procured or used to process PII without prior approval from M/CIO (see **ADS 509**, **ADS 331**, and **Software and Hardware Requests (SHR)** for additional guidance).

Agency Activity Planner, COs, and CORs must work with General Counsel, Program Managers, System of Records Managers, and SOs to include appropriate privacy protection language in terms of service and contracts (see **ADS 545** and **ADS 302mah**) to:

1. Limit the right of the cloud services provider to change the negotiated terms of service (TOS) at will if the changes would affect any USAID rights or obligations. Any proposed changes to the terms of service that could alter the privacy risks during the life of the contract must be reviewed by General Counsel (see **ADS 302mah** and **ADS 558** for guidance on social media channels); and

2. Limit the right of the cloud services provider to change the location where the PII is stored and processed, because data located outside of the United States could be subject to data protection requirements significantly different from those of the United States, and location changes may require amendment of privacy compliance documentation such as PIAs and SORNs.

The way a cloud services provider addresses privacy concerns within their environment may affect the overall price and technical structure for a proposed cloud computing solution (*i.e.,* how the data is encrypted while in transit and while being stored (*i.e.,* at rest) on their servers). The Activity Planner in B/IO/Ms must work with the Privacy Program to identify privacy requirements as early as possible in the information lifecycle to understand

how USAID will require that a cloud services provider maintains its duty to protect PII, as well as the funding implications of doing so.

The Federal Risk and Authorization Management Program (**FedRAMP**) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. **FedRAMP Control Specific Contract Clauses version 3.0** includes some appropriate privacy requirements for cloud computing contracts.

For additional information on cloud computing, see **Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service**, a resource published by the CIO Council.

c. Computer Matching Programs and Agreements

Computer matching programs are computerized comparisons of two or more automated systems of records for the purposes of: (i) establishing or verifying eligibility for a Federal benefit program; and (ii) recouping payments or delinquent debts under such programs. Matching programs may also compare Federal systems of records and personnel or payroll systems with non-Federal systems of records and personnel or payroll systems. To ensure that Federal agencies use computer matching appropriately, the **Computer Matching and Privacy Protection Act of 1988 (CMPPA)** requires agencies to give notice before taking action based on a match. When USAID participates in matching programs, the Data Integrity Board must oversee computer matching programs. Workforce members must not disclose any records contained in a system of records to a recipient agency for use in a computer matching program, except in compliance with a written agreement between USAID and the recipient agency.

For more information on matching programs and agreements, see **5 USC 552a(o)** and **OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy** (see section **508.3.5.14**).

508.3.4.10 Privacy Reporting

Effective Date: 01/11/2022

The USAID SAOP reports the SAOP Federal Information Security Management Act (FISMA) metrics to OMB annually. The report includes OMB defined metrics, which may vary from year to year. The SAOP also responds to congressional inquiries on an ad hoc basis.

a. Privacy Breach Reporting and Response

USAID must manage the information it processes in support of its Mission and business functions, in accordance with Federal laws and regulation. Any unauthorized use, disclosure, or loss of such information can result in the loss of

the public's trust and confidence in the Agency's ability to protect it properly. PII breaches may have far-reaching implications for individuals whose PII is compromised, including identity theft resulting in financial loss and/or personal hardship. Although most incidents involve information technology, a privacy breach may also involve physical security considerations (*e.g.,* paper documents, removable media, and mobile devices).

All members of the workforce operating on behalf of USAID must report immediately and without delay upon suspicion or discovery of any incident that may be a potential suspected or actual privacy breach to the M/CIO Service Desk at USAID Service Central at **cio-helpdesk@usaid.gov** or (202) 712-1234 and the Privacy Program at **privacy@usaid.gov**, regardless of the format of the PII compromised (*i.e.,* oral, paper, or electronic) or the manner in which the incidents might have occurred.

OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" requires all federal agencies to report privacy incidents to the **United States Computer Emergency Readiness Team (US-CERT)**. USAID's **Privacy Program Breach Notification and Response Plan** outlines the Standard Operating Procedures for the USAID Breach Response Team's (BRT) approach for coordinating a response to a privacy incident.

Consistent with Agency policy, the USAID CSIRT must report suspected and/or confirmed breaches to the US-CERT, as instructed by the Department of Homeland Security (DHS) and OMB.

The USAID Privacy Incident Response Team (PIRT) within the Privacy Program evaluates the incident. If PIRT determines that USAID should report the incident to US-CERT, the Privacy Program submits a report to the USAID CSIRT. If the incident warrants reporting to US-CERT, in accordance with **US-CERT Federal Incident Notification Guidelines**, CSIRT must report the incident to the US-CERT within one hour of discovery.

Depending on the level and suspected impact of the breach, PIRT will notify the BRT, which will decide how the Agency will respond to breaches of sensitive PII, including whether notification to affected individuals and/or credit monitoring are warranted. The Agency's BRT is a group of Agency officials that the SAOP may convene in the event of a major incident. BRT is responsible for advising the head of the Agency on how to effectively and efficiently respond to a breach. Decisions and recommendations are made by consensus. In addition, the BRT members must participate in an annual tabletop exercise.

At a minimum, the Agency's BRT must include:

- The SAOP;

- The CPO;
- The CIO or the Deputy CIO;
- The CISO;
- GC;
- LPA; and
- A representative of the responsible B/IO/M.

OMB M-17-12, defines the following terms:

Incident: An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.

Major Incident: A breach that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

The Privacy Program Privacy Breach SOP defines the major incident threshold for the Agency. The document is available to users with a need to know by emailing the Privacy Program at **privacy@usaid.gov**.

The most common privacy breaches occur when personal information of customers, clients, or employees is lost, stolen, or mistakenly disclosed. For example, a PII breach could involve a lost or stolen laptop or mobile device containing PII, mistakenly sending an unencrypted email containing PII to the wrong person, or misplacing or losing paper files, etc.

b. Open Government and Open Data

In compliance with the **Executive Order 13642 of May 9, 2013, Making Open and Machine Readable the New Default for Government Information** and **OMB Memorandum M-13-13, Open Data Policy-Managing Information as an**

Asset, USAID must implement tools and processes that accelerate the access, use, and public availability of Federal information. While USAID is guided by the principle of "open by default," the Agency must ensure that adequate policy, process, and technical safeguards are in place to prevent the inappropriate disclosure of PII. For more information, see **ADS Chapter 579, USAID Development Data**.

The OU that funded the dataset must complete an Open Data Privacy Analysis (ODPA) template located on the internal **USAID Privacy page** before the dataset is posted to a public website, and thereafter periodically, before updating datasets on websites available to the public.

The Privacy Program uses the completed USAID ODPA template to determine whether a particular dataset involves privacy risks and to identify what privacy protection actions the program must take before it posts the dataset on a website available to the public. The CORs/AORs responsible for the dataset in the program must assess whether a particular dataset contains PII and must comply with all privacy protection requirements, such as removing PII from the dataset and any sensitive metadata associated with that dataset, before posting the dataset to a website available to the public.

For more information on AOR/COR responsibilities for Open Data, see **ADS 579**.

508.3.4.11 Restriction on Mailing Documents Containing Social Security Numbers and PII

Effective Date: 01/11/2022

In accordance with the **Social Security Number Fraud Prevention Act of 2017 (Pub. L. 115-59)**, documents containing SSNs or other PII may only be sent by U.S. mail as a last resort. In rare circumstances in which documents with SSNs or PII must be sent by U.S. mail, the guidelines below must be followed:

- The head of the agency (or designee) must review and determine that the inclusion of the SSN on the document is necessary;
- The SSN or PII must not be visible on the outside of any mail;
- The pages containing PII must be double wrapped and sent by the U.S. Postal Service (USPS) or a commercial delivery service (*e.g.,* FedEx, DHL). All services must provide tracking and delivery confirmation; and
- Packages that contain SSN or PII that are mailed to posts abroad must be sent via unclassified registered pouch or to a Military Postal Facility (MPF) via USPS, whenever practicable. Use of foreign mail services is authorized, if required. Except in those cases where the pouch is used, mail must be packaged in a way that does not disclose its contents.

For additional guidance on handling documents with SSNs or PII (such as those with a partial redaction of the SSN or PII), please contact the Privacy Program at **privacy@usaid.gov**. Please contact the Bureau for Management, Office of Management Services (M/MS) for guidance on mailing materials at **facilities@usaid.gov**.

508.3.4.12 Annual PII Inventory
Effective Date: 01/11/2022

The USAID Privacy Program must review its PII holdings at a minimum annually and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete and reduce them to the minimum necessary for the proper performance of a documented USAID function. The USAID Privacy Program conducts an inventory that aims to provide a basis for the Agency's overall privacy footprint. This PII inventory survey requires input from USAID's B/IO/Ms and serves as a baseline to evaluate USAID PII processing and to identify areas where PII holdings can be reduced or eliminated.

508.3.4.13 PII Retention and Disposal
Effective Date: 01/11/2022

All members of the workforce must carefully store and destroy PII and media containing PII on the approved disposition date using USAID-approved methods. Members of the workforce must secure PII in documents or on media within a locked office or suite, or secure them in a locked container (*e.g.,* file cabinet). Members of the workforce must destroy PII documents by shredding and must store and destroy media containing PII in accordance with methods described in **ADS 545**'s section on media handling, and **ADS 545mas, Media Handling Procedures and Guidelines**.

Members of the workforce must retain and dispose of PII in accordance with **National Archives and Records Administration General Records Schedules** and USAID-approved disposition schedules (see **ADS 502**).

508.3.5 USAID Privacy Risk Mitigation Requirements
Effective Date: 01/11/2022

USAID takes data privacy protection very seriously and complies with multiple Federal privacy regulations. However, regulations are not always enough to ensure best practices are consistently followed. USAID employs the following measures to ensure robust privacy practices are incorporated throughout Agency functions that are not addressed by specific laws and regulations.

508.3.5.1 Privacy Review of Software and Hardware for Agency Use
Effective Date: 01/11/2022

If a B/IO/M needs software or hardware that is not on the **Agency's Approved Product Catalog**, the B/IO/M must submit a **Software and Hardware Request (SHR)** to M/CIO

for consideration (see the **Approved Product Catalog Guide** for guidance on submitting a SHR). The Privacy Program must review the requested software or hardware for potential privacy risks and provide recommendations based on the privacy assessment. B/IO/Ms are prohibited from purchasing equipment that is not approved by M/CIO.

508.3.5.2 Privacy Awareness Training
Effective Date: 01/11/2022

All members of the USAID workforce or others working on behalf of the Agency accessing USAID systems must receive initial USAID training in security and privacy awareness and accepted security and privacy practices. Members of the workforce must complete security and privacy literacy and awareness training and review and sign the **ADS 545mdb, Rules of Behavior for Users** before obtaining a user account with logical AIDNet access and active directory accounts.

Additionally, all USAID personnel must complete annual refresher training in security and privacy literacy and awareness. Members of the USAID workforce must complete security and privacy literacy and awareness within the first year of being granted a user account and review and acknowledge the Rules of Behavior (ROB) annually thereafter.

Training non-compliance escalation may result in all system accounts, including access to email being limited and/or disabled for users who do not comply with training requirements. In limited cases, extensions, not waivers or exemptions, may be granted in writing by the CISO; however, these cases must be justified, documented, and approved by the individual's supervisor.

Subsequent security and privacy literacy and awareness training may be required to address changes to the system, policy changes to security and privacy, or increasing threat attacks.

M/CIO/IA also provides targeted role-based training to individuals responsible for PII or activities that involve PII. U.S. Direct-Hire supervisors may request additional role-based privacy literacy and awareness training by emailing **privacy@usaid.gov**.

See the **ADS 545** sections titled ROB IT Security Training and Information Security Awareness, Training, and Education, for more information about IA training, and see **ADS 545mbd** for more information about ROB.

508.3.5.3 Automating Privacy Controls
Effective Date: 01/11/2022

USAID employs technologies and system capabilities to automate privacy controls. By building privacy controls into system design and development, USAID mitigates risks to PII, thereby reducing the likelihood of breaches and other privacy-related incidents. USAID regularly monitors system use and the sharing of PII to ensure processing is

consistent with the authorized purposes identified in the Privacy Act and/or in the public notices issued, or in a manner compatible with those purposes.

508.3.5.4 PII Use for System Testing, Training, and Research

Effective Date: 01/11/2022

The use of identifiable PII in testing, training, and research increases the risks of unauthorized disclosure or misuse of such PII. SOs and PMs are not authorized to use identifiable PII during system testing, training, or research and must take measures to eliminate PII from data used for such purposes. For more information on protecting PII, see **NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**.

508.3.5.5 Social Security Number Use Reduction and Elimination

Effective Date: 01/11/2022

The Privacy Program focuses on the reduction and elimination of USAID's dependence on SSNs because of the elevated risk of harm to individuals from the compromise of SSNs. USAID may only collect and use SSNs where there is a legal authority to do so. USAID must review its use of SSNs in Agency systems and programs to identify instances in which collection or use of the SSN is superfluous and must reduce or eliminate its use of SSNs.

The Privacy Program developed a working group with key stakeholders to review the use of and reduce USAID's reliance on SSNs. Reducing Agency SSN processing decreases the risk to individuals of potential identity theft if systems are compromised. The Privacy Program works with forms owners, System of Records Managers, and SOs to reduce the volume of processed SSNs to the minimum necessary to accomplish a business function and to limit the number of workforce members who have access to SSNs to only those with a need to know to complete their job functions. For more information on SSN use reduction and elimination, see **OMB M-17-12**.

508.3.5.6 Data Quality and Integrity

Effective Date: 01/11/2022

SOs and/or members of the workforce processing data must take reasonable steps to protect the quality, timeliness, relevance, and integrity of the processed PII. All employees are responsible for using PII properly. This includes maintaining the quality and integrity of all processed PII. See **ADS Chapter 578, Information Quality Guidelines** and **ADS 597sad, Data Quality Assessment Checklist** for more information about data quality.

PMs, System of Records Managers, and SOs must validate PII that is obtained from sources other than the subject individuals or the authorized representatives of such individuals. This is necessary to ensure fairness in any determination about an individual and promotes the FIPPs of data quality and integrity.

USAID SOs must also implement security and privacy controls to maintain the accuracy and consistency of PII throughout the data lifecycle. This is necessary to ensure fairness in any determination about an individual and promote FIPPs.

508.3.5.7 Security Controls for Personally Identifiable Information

Effective Date: 01/11/2022

Because it is SBU information, PII requires greater controls against unauthorized access and disclosure than other information that is Unclassified. Workforce members must label documents containing PII with the SBU header and footer and use the green SBU cover sheet with paper documents. Workforce members must protect PII, as well as other SBU information, against unauthorized access or disclosure by ensuring that only people who have a clearly demonstrated need to know to use the information are given access.

FISMA requires that each agency implements a comprehensive security program to protect the agency's information and information systems. SOs and ISSOs, in coordination with the M/CIO/IA, must implement the catalog of security and privacy controls in **NIST SP 800-53, Rev. 5**, which provides safeguards and countermeasures for USAID information and information systems. SOs and ISSOs apply security and privacy controls to protect against the loss, unauthorized access, or unauthorized disclosure of PII.

508.3.5.8 Encrypting PII

Effective Date: 01/11/2022

Under **OMB Circular A-130** and security controls in **NIST SP 800-53, Rev. 5**, SOs and ISSOs must ensure that all PII is encrypted when at rest, in motion, during remote and wireless access, and on all removable media, such as laptops and other devices (*e.g.,* iPads and iPhones).

Workforce members must not email PII from a usaid.gov email address without protecting the PII. Individuals must remove all PII from email strings, including in screenshots and other images, and must encrypt all PII in email attachments, whether sent to a .gov address or another email domain. In addition, individuals must ensure that PII is encrypted on all removable media (*e.g.,* CDs, DVDs, and thumb drives) and not shared within collaborative sites. For more information about encrypting PII, see **ADS 545** and **ADS 545mbd**. Additionally, see the **Agency Notice, Mandatory Encryption of Email Attachments Containing PII**.

508.3.5.9 Remote Access to PII

Effective Date: 01/11/2022

When working remotely, members of the workforce must use a USAID-issued electronic device or an RSA-token-enabled connection (**remoteaccess.usaid.gov**) when they collect, use, maintain, and disseminate PII. For more information about remote access

requirements, see **ADS 545**, **ADS Chapter 549, Telecommunications Management**, and **ADS Chapter 405, Telework**.

508.3.5.10 Access to Electronic Records of Former Employees

Effective Date: 01/11/2022

USAID may provide access to the electronic records (*i.e.,* emails, documents, and mobile devices) of former employees to supervisors of former employees, or any workforce member delegated by such supervisor, for business and/or legal purposes only. The appropriate Administrative Management Services (AMS) Officer must authorize the approval of a valid need to know.

508.3.5.11 Individual Participation, Redress, and Complaint Management

Effective Date: 01/11/2022

Participation includes consent and access to PII by the subject individual. Redress includes amendment of the PII and disseminating PII corrections to external partners with whom USAID shares the PII. Complaint management includes receiving and responding to complaints, concerns, or questions about organizational privacy practices. OIG is responsible for administering FOIA and the **Privacy Act** with respect to its own records.

The Privacy Program is responsible for responding to privacy complaints submitted by individuals, both internal and external to USAID, including the USAID workforce, the public, other government agencies, USAID partners, and the private sector. The Privacy Program investigates privacy complaints pursuant to the **Privacy Act** and the **Freedom of Information Act (FOIA)** related to records about individuals (*i.e.,* U.S. citizens and lawfully admitted permanent resident aliens).

508.3.5.12 Use Limitation

Effective Date: 01/11/2022

USAID must only use PII as specified in their public notices and in a manner compatible with those specified purposes, or as otherwise permitted by law. Members of the workforce must follow ROB regarding the protection of PII or may be subject to the penalties enumerated in the Privacy Act and/or disciplinary actions. In addition, USAID should share PII only as authorized by law or for the authorized purposes in the Privacy Act and routine uses published in the appropriate SORN or Privacy Act Statement or notice. For more details on the privacy responsibilities of workforce members, see **ADS 545mbd**.

508.3.5.13 Internal Use

Effective Date: 01/11/2022

USAID must use PII internally only for the authorized purposes identified in the Privacy Act and the appropriate purposes stated in the USAID SORN that covers the specific PII

involved. In addition, individuals are authorized to use specific PII only when they have the need to know to comply with their job responsibilities.

508.3.5.14 Sharing PII with Third Parties

Effective Date: 01/11/2022

Sharing PII with third parties is the same as disclosing PII to third parties. Third parties can be organizations or persons. B/IO/Ms must only share PII with third parties as authorized by the Privacy Act and the appropriate Routine Uses in the USAID SORN that covers the specific PII involved.

Where appropriate to share PII with third parties, B/IO/Ms must enter into a memorandum of understanding (MOU), a memorandum of agreement (MOA), a letter of intent, a computer matching agreement, a nondisclosure agreement, or similar agreement with that third party. The agreement must specifically state the authority for sharing the information, the safeguards required for retention of the data, the purposes for which the PII may be used, as well as disclosures, if any, that may be made and retention conditions. For more information on sharing PII with third parties, see **OMB Memorandum M-01-05** and **OMB Memorandum M-11-02, Sharing Data While Protecting Privacy**.

508.3.5.15 Data Loss Prevention (DLP)

Effective Date: 01/11/2022

Both Federal and USAID policy requires PII to be protected from loss, disclosure, or any other unauthorized use. The Privacy Program is responsible for providing the requirements for a DLP program. DLP refers to a family of capabilities consisting of policies, technologies, and configurations designed to safeguard the Agency's information from unauthorized access, alteration, or destruction.

The USAID DLP program must include a combination of people, processes, and technology to meet its goals, which include effective data handling procedures, using tools to monitor and control data leaving the Agency, investigating possible violations of Agency data handling policies, providing remedial training to violators, or referring them for disciplinary action, and providing management feedback on the effectiveness of the DLP program.

The Privacy Program must formulate the functional requirements for DLP technologies. The Privacy Program works with the DLP implementation team to monitor and determine the effectiveness of the requirements in protecting data and minimizing issues created by the DLP tools, such as delays in information dissemination and business interruption.

The USAID Privacy Program may provide remedial training to USAID workforce members and contractors who make isolated and unintentional policy violations.

508.4 MANDATORY REFERENCES

508.4.1 External Mandatory References

Effective Date: 01/11/2022

a. 12 FAM 540, Sensitive But Unclassified Information (SBU)

b. 22 CFR 215, Regulations For Implementation of Privacy Act of 1974

c. Administrative Procedure Act of 1946, as amended at 5 USC 553, Rule Making

d. Children's Online Privacy Protection Act of 1998, as amended at 15 USC 6501-6506, Children's Privacy

e. Confidential Information Protection and Statistical Efficiency Act of 2002, as amended at 44 USC 3501 note

f. Consolidated Appropriations Act 2005, as amended at 42 USC 2000ee-2

g. Consolidated Appropriations Act, 2016 (Cybersecurity Act of 2015 [P.L. 114-113, Division N])

h. E-Government Act of 2002, Section 208, as amended at 44 USC 3501 note

i. Executive Order 13402, Strengthening Federal Efforts to Protect Against Identity Theft

j. Executive Order 13414, Amendment to Executive Order 13402, Strengthening Federal Efforts to Protect Against Identity Theft

k. Executive Order 13642, Making Open and Machine Readable the New Default for Government Information

l. Executive Order 14035, Diversity, Equity, Inclusion and Accessibility in the Federal Workforce

m. Federal Acquisition Regulation (FAR) (48 CFR) Part 24, Protection of Privacy and Freedom of Information

n. Federal Acquisition Regulation (FAR) (48 CFR) 52.239–1 Privacy or Security Safeguards

o. Federal Information Security Modernization Act of 2014

p. Government Paperwork Elimination Act of 1998, as amended at 44 USC 3504 note

q. Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191)

r. NIST FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems

s. NIST Privacy Framework

t. NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

u. NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations

v. NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide

w. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

x. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing

y. OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," July 2017

z. OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act"

aa. OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control"

ab. OMB Circular A-130, "Managing Information as a Strategic Resource"

ac. OMB Memorandum M-01-05, "Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy"

ad. OMB Memorandum M-03-18, "Implementation Guidance for the E-Government Act of 2002"

ae. OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"

af. OMB Memorandum M-05-08, "Designation of Senior Agency Officials for Privacy"

ag. OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments"

ah. OMB Memorandum M-10-06, "Open Government Directive"

ai. OMB Memorandum M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies"

aj. OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications"

ak. OMB Memorandum, "Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications"

al. OMB Memorandum M-11-02, "Sharing Data While Protecting Privacy"

am. OMB Memorandum M-13-13, "Open Data Policy–Managing Information as an Asset"

an. OMB Memorandum M-13-20, "Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative"

ao. OMB Memorandum M-13-21, "Implementation of the Government Charge Card Abuse Prevention Act of 2012"

ap. OMB Memorandum M-14-06, "Guidance for Providing and Using Administrative Data for Statistical Purposes"

aq. OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information"

ar. OMB Memorandum M-99-05, Attachment B, "Instructions on Complying with President's Memorandum of May 14, 1998, 'Privacy and Personal Information in Federal Records'"

as. Paperwork Reduction Act of 1995, as amended at 44 U.S.C 3501-3521 (P.L. 104-13)

at. Privacy Act of 1974, as amended at 5 U.S.C Section 552a

508.4.2 Internal Mandatory References

Effective Date: 07/06/2022

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 303, Grants and Cooperative Agreements to Non-Governmental Organizations

e. ADS 306, Interagency Agreements

f. ADS 331, USAID Worldwide Purchase Card Program

g. ADS 405, Telework

h. ADS 485, Disciplinary Action - Foreign Service

i. ADS 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct - Civil Service

j. ADS 502, The USAID Records Management Program

k. ADS 502mah, Policies and Procedures for Recording Audio and Video Meetings

l. ADS 505, Forms Management Program

m. ADS 506, Reports Management

n. ADS 507, Freedom of Information Act (FOIA)

o. ADS 508mag, USAID Privacy Act Section (e)(3) Statement or Notice Template

p. ADS 508mak, USAID Public Website Privacy Policies Requirements

q. ADS 508mai, USAID Privacy Program Breach Notification Policy and Response Plan

r. ADS 509, Management and Oversight of Agency Information Technology Resources

s. ADS 516, Federal Register Notices

t. ADS 545, Information Systems Security

u. ADS 545mbd, Rules of Behavior for Users

v. **ADS 549, Telecommunications Management**

w. **ADS 557, Website Management and Public Information**

x. **ADS 578, Information Quality Guidelines**

y. **ADS 579, USAID Development Data**

z. **ADS 596mab, Governance Charter for Enterprise Risk Management and Internal Control at USAID**

aa. **ADS 597sad, Data Quality Assessment Checklist**

bb. **ADS 626mab, Contractors Functioning as Timekeepers**

ab. **USAID SDLC Development Framework** (Note: This link can only be accessed on the USAID network.)

508.5 ADDITIONAL HELP

Effective Date: 01/11/2022

a. **ADS 508saa, Privacy Basics**

b. **Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service**

c. **FedRAMP Control Specific Contract Clauses**

d. **USAID Plan to Respond to Breaches of Privacy**

508.6 DEFINITIONS

Effective Date: 01/11/2022

See the **ADS Glossary** for all ADS terms and definitions.

Access
The ability and opportunity to obtain knowledge of classified information. An individual is considered to have access by being in a place where national security information is kept, processed, handled, or discussed, if the security control measures that are in force do not prevent that person from gaining knowledge of such information. (**Chapters 508, 566, 569**)

Access to Records
Giving members of the public, at their request, Federal Agency records to which they are entitled by a law (*e.g.,* Privacy Act or the Freedom of Information Act). (**Chapter 508**)

Breach
The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for any reason other than its authorized purpose. (**Chapter 508**)

Cloud Computing
Internet-based computing whereby shared resources, software, and information are provided to computers and other devices. (**Chapter 508**)

Data Loss Prevention (DLP)
Data loss prevention (DLP) is a set of tools and processes used to ensure that sensitive and/or confidential data, including PII, is not lost, misused, or accessed by unauthorized users. DLP software identifies and categorizes Classified, SBU, confidential and other sensitive data and identifies violations of Agency policies. Once violations are identified, DLP enforces remediation with alerts and other protective actions to prevent users from accidentally or maliciously sharing data that could put the organization at risk. DLP also provides reporting mechanisms to meet compliance and auditing requirements and supports the identification of vulnerabilities for incident response. (**Chapter 508**)

Dataset
An organized collection of structured data, including data contained in spreadsheets, whether presented in tabular or non-tabular form (*e.g.,* a dataset may represent a single spreadsheet, an extensible mark-up language [XML] file, a geospatial data file, or an organized collection of these). (**Chapter 508** and **579**)

Disclosure
Dissemination or communication of any information that has been retrieved from a protected record by any means of communication (*i.e.,* written, oral, electronic, or mechanical) without written request by or consent of the individual to whom the record pertains. (**Chapter 508**)

Dissemination of Information
Actively distributing information to the public at the initiative of the Agency. (**Chapter 508**)

Encryption
The act of transforming information into an unintelligible form, specifically to obscure its meaning or content. (**Chapter 508** and **545**)

Federal Benefit Program
Any program administered or funded by the Federal Government, or by any agent or state on its behalf, that provides cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals. (**Chapter 508**)

Incident
See privacy incident. (**Chapter 508**)

Individual
A citizen of the United States or an alien lawfully admitted for permanent residence. (**Chapter 508**)

Information Collection
Obtaining, soliciting, or requiring the disclosure to third parties or the public of facts or opinions by or for an agency, regardless of form or format (*e.g.,* requesting responses from 10 or more people other than Federal employees or agencies, which are to be used for general statistical purposes). This usage does not include collection of information in connection with a criminal investigation or prosecution. (**Chapter 508**)

Information in Identifiable Form (IIF)
Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means (same as PII). (**Chapter 508**)

Information Lifecycle
The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition. (**Chapter 508** and **545**)

Information System
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.) (**Chapters 502, 508, 509, 545, 620**)

Information System Security Officer (ISSO)
Individuals responsible to the senior Agency information security officer, the AO, or the information SO for ensuring the appropriate operational security posture is maintained for an information system or program. (**Chapter 508** and **545**)

Interagency Agreement
Any agreement between two Federal agencies by which one agency buys goods or services from the other, including but not limited to an agreement under the authority of the Federal Aviation Administration (FAA) section 632(b), the **Economy Act of 1932**, the **Government Management Reform Act of 1994** or similar legislation, or by which one agency transfers or allocates funds to another under the authority of FAA section 632(a). (**Chapters 300, 306, 508**)

Maintain
Collection, use, updating, sharing, disclosure, dissemination, transfer, and storage of PII. (**Chapter 508**)

Major Incident
A breach that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. The Privacy Program Privacy Breach SOP defines the major incident threshold for the Agency. (**Chapter 508**)

Matching Agreement
The agreement that establishes the terms of a matching program between USAID and another Federal or non-Federal agency. (**Chapter 508**)

Matching Program
A computerized comparison of two or more automated systems of records, or an SOR with non-Federal records. (**Chapter 508**)

Paperwork Reduction Act (PRA)
This legislation was passed to minimize the paperwork burden and ensure greatest public benefit from information collected by or for the Federal Government. Other purposes for this law include minimizing costs, improving the quality, use, and dissemination of information collected, consistent with all applicable laws. (**Chapter 508**)

Personal Identifier
A name, number, or symbol that is unique to an individual (*e.g.,* an individual's name and SSN). It may also include fingerprints or voiceprints. (**Chapter 508**)

Personally Identifiable Information (PII)
Per **OMB A-130**, PII 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 could 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**)

Policy
USAID policy includes both mandatory guidance (*i.e.,* policy directives and required procedures and internal mandatory references) and broader official statements of Agency goals, guiding principles, and views on development challenges and best practices in addressing those challenges. (**Chapter 501** and **508**)

Privacy Act Record
Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history. The record contains the name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. (**Chapter 508**)

Privacy Act Request
A request from an individual for notification as to the existence of, access to, or amendment of records about that individual. These records must be maintained in a system of records and the request must indicate that it is being made under the Privacy Act to be considered a Privacy Act request. (**Chapter 508**)

Privacy Act Statement
A statement, required by the **Privacy Act, Section (e)(3)**, appearing on a website or information collection form which notifies the users of the authority for collecting requested information. It also states the purpose and use of the collected information. USAID must notify the public or users if providing such information is voluntary or mandatory, and the effects, if any, of not providing all or any portion of the requested information (see also Privacy Act Statement). (**Chapter 508)**

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 Incident
A violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices, involving the breach of PII, whether in electronic or paper format. (**Chapter 508**)

Privacy Notice
A statement made to a data subject that describes how the organization collects, uses, retains, and discloses personal information. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement, or sometimes a privacy policy. (**Chapter 508**)

Privacy Threshold Assessment (PTA)
A PTA provides a high-level description of an information system including the information it contains and how it is used. The PTA determines and documents whether or not a PIA is required. (**Chapter 508** and **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 GLAAS. (**Chapters 300, 508, 545, 629**)

Recipient Agency
Any agency, or its contractor, that receives records contained in a system of records from a source agency for use in a matching program. (**Chapter 508**)

Record
See Privacy Act record. (**Chapter 508**)

Routine Use
With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected. (**Chapter 508**)

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

SBU information includes, but is not limited to:

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

- Information offered under conditions of confidentiality which arises in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers. (**Chapters 508, 545, 562, 566**)

Servicing Agency
The Federal Agency that provides goods or services to another agency under the authority of the Economy Act or similar legislation. (**Chapter 306** and **508**)

Significant Change

Defined as a change that is likely to affect the security state of an information system. Significant changes to an information system may include (1) the installation of a new or upgraded operating system, middleware component, or application; (2) modifications to system ports, protocols, or services; (3) the installation of a new or upgraded hardware platform; (4) modifications to cryptographic modules or services; or (5) modifications to security controls. For the purposes of privacy compliance, significant changes are applicable when they are a change that is likely to affect the privacy risks of the PII in the system. (**Chapter 508**)

Source Agency
Any agency (including state or local government) that discloses records contained in a system of records to be used in a matching program. (**Chapter 508**)

Supervisor
Employees responsible for the "direction" of subordinates within their organization unit and whose supervisory responsibilities meet at least the minimum requirements for coverage under the **General Schedule Supervisory Guide**. Those directed may be subordinate Federal civil service employees; assigned military employees; non-Federal workers; unpaid volunteers; student trainees; or others. Supervisors serve as coaches that empower staff to accomplish work. Traditional supervisory duties include evaluating employee performance; selecting or participating with considerable weight in the selection of subordinate employees; reviewing and approving leave requests; hearing and resolving complaints and grievances; and effecting disciplinary measures. (**Chapters 405, 413, 508**)

System
Any information system or application. The term may be used to designate both the hardware and software that comprise it. (**Chapter 508** and **545**)

System of Records
A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. (**Chapter 508**)

System of Records Manager
Individual responsible for the daily program and operational management of their specific USAID Privacy Act system of records. System of Records Managers are responsible for ensuring that their system of records and the related USAID program comply with the requirements of the Privacy Act. (**Chapter 508**)

System of Records Notice
A notice of the existence and character of the system of records; the notice must include (1) the name and location of the system; (2) the categories of individuals on whom records are maintained in the system; (3) the categories of records maintained in the system; (4) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (5) the policies and practices of the

agency regarding storage, retrievability, access controls, retention, and disposal of the records; (6) the title and business address of the agency official who is responsible for the system of records; (7) the agency procedures whereby individuals can be notified at their request if the system of records contains a record pertaining to them; (8) the agency procedures whereby individuals can be notified at their request how they can gain access to any record pertaining to them contained in the system of records, and how they can contest its content; and (9) the categories of sources of records in the system (**Chapter 508**)

System Owner (SO)
Individuals responsible for daily program and operational management of their specific USAID system. SOs are responsible for ensuring that a security plan is prepared, implementing the plan, and monitoring its effectiveness. (**Chapter 508** and **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. (**Chapter 405** and **508**)

Third-party Websites and Applications
Web-based technologies that are not exclusively operated or controlled by a government entity. Often, these technologies are located on a .com website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official website. (**Chapter 508**)

Unauthorized Disclosure
When PII is disclosed to anyone except the subject individual absent, the written consent of the subject individual is required, unless the disclosure falls within one of 12 statutory conditions in the **Privacy Act, 5 U.S.C 552a(b)(1)-(12)**. (**Chapter 508**)

Workforce
All individuals working for or on behalf of the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems. This includes, but is not limited to, U.S. Direct-Hire employees, personal services contractors, fellows, interagency personnel, and contract personnel. (Note: Contractors are not normally subject to Agency policy and procedures as discussed in **ADS 501.1**. However, contract personnel are included here by virtue of the applicable clauses in the contract related to **HSPD-12** and information security requirements.) (**Chapters 508, 545, 547, 552**)

508_021623