
# ADS Chapter 508

# Privacy Program

Partial Revision Date: 08/31/2020
Responsible Office: M/CIO/IA
File Name: 508_083120

**Functional Series 500 – Management Services**
**ADS 508 – Privacy Program**
**POC for ADS 508: William Morgan, wmorgan@usaid.gov, (571) 218-0829**

## Table of Contents



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

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

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

## 508.1 OVERVIEW

Effective Date: 08/31/2020

This ADS chapter codifies and provides the organization, functions, policies, and procedures contained within the USAID Privacy Program.

Safeguarding Personally Identifiable Information (PII) (see **508.3.1**) and preventing its misuse are essential to ensure that USAID retains the trust of the American public. USAID's responsibility to the American public is a function of the **Privacy Act of 1974** and the federal privacy authorities that followed it, including the **E-Government Act of 2002, Section 208**.

USAID must establish appropriate safeguards to ensure the security and confidentiality of records and to protect PII against anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To accomplish that requirement, USAID must incorporate privacy analyses into each stage of the information lifecycle.

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 with the rights of individuals to be protected against unwarranted invasions of their privacy resulting from the collection, maintenance, use, and dissemination of their personal information.

The Privacy Team under the Office of the Chief Information Officer (M/CIO/OCIO) monitors federal privacy laws and policy for changes that affect the privacy program and develops a strategic privacy plan to implement applicable policies, procedures, and privacy controls. The Privacy Team reviews or updates the Agency privacy plan, policies, and procedures at least annually.

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

Throughout this chapter, the term "workforce" refers to individuals working for or on behalf of the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems. This includes Direct-Hire employees, Personal Services Contractors, Fellows, Participating Agency Service Agreement and 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 details on the USAID Privacy Program, see **http://www.usaid.gov/privacy**.

This document does not cover policies related to Section 508 of the Rehabilitation Act, 29 USC 794d, as amended. For information about federal agency compliance with Section 508, see **http://www.section508.gov/**. For information about USAID Section 508 requirements for Agency acquisitions see **ADS 302mak, USAID Implementation of Section 508 of the Rehabilitation Act of 1973**.

## 508.2 PRIMARY RESPONSIBILITIES

Effective Date: 07/30/2019

For additional information and answers to basic questions about the responsibilities to protect PII, see **ADS 508saa, Privacy Basics**.

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

**b.** The **Senior Agency Official for Privacy (SAOP)** has overall responsibility and accountability for ensuring the Agency's implementation of privacy protections, including USAID's full compliance with federal laws, regulations, and policies relating to privacy. The SAOP must ensure that the Agency Data Loss Prevention (DLP) Program has adequate staffing, processes, and technical tools to implement DLP requirements.

**c.** The **Bureau for Management, Office of the Chief Information Officer (M/CIO)** in the Bureau for Management, (M/CIO) is responsible for the oversight of the Agency's Information Resource Management, as defined in the E-Government Act of 2002 and OMB Circular A-130; the purchasing and supervision of the Agency's information-technology resources, as defined in OMB Circular A-130 and the FITARA; as well as all functions mandated by the Clinger-Cohen Act of 1996 and FITARA.

**d.** The **Chief Privacy Officer (CPO)** is designated by the Assistant Administrator, Bureau for Management (M/AA) and provides oversight and guidance for privacy policy and procedures, compliance activities, reporting, and the effectiveness of the Agency-wide Privacy Program, as well as ensuring that privacy requirements are incorporated into each stage of the information lifecycle. The CPO ensures that DLP processes are developed and implemented to protect Sensitive But Unclassified (SBU) and PII electronic and hardcopy data and to mitigate risks to USAID business operations from privacy data loss.

**e.** The **Privacy Program** 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, such as Privacy Threshold Analyses, Privacy Impact Assessments, Privacy Act Statements on USAID Forms, and Systems of Records Notices; privacy awareness training to employees; privacy incident analysis and privacy breach response recommendations; and coordinating with USAID officials and employees on privacy protection and compliance activities.

**f.** The **Chief Information Security Officer (CISO)** is designated by the Chief Information Officer 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 M/CIO/ITO to implement DLP architecture and/or enterprise configurations.

**g.** The **Computer Security Incident Response Team (CSIRT) (M/CIO/IA)** coordinates and supports the response to a computer security event or incident. CSIRT handles all computer security and Classified Spillage incidents for USAID and works with privacy to address PII related incidents. CSIRT is the central reporting authority to U.S.-Computer Emergency Readiness Team (U.S.-CERT). CSIRT Analysts investigate, resolve, and report DLP security violations to the U.S.-CERT.

**h.** The **M/CIO Security Operations Center (SOC)** investigates incidents created by the Agency Data Loss Prevention (DLP) for false positives, and interdicts non-encrypted emails containing PII by placing them in quarantine. The SOC ensures that end users do not send sensitive or critical information outside the USAID network. The CSIRT Team, which is the specialized response team in the SOC, addresses incidents through the use of the DLP tools.

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

Additionally, M/MS/IRD is responsible for managing USAID's compliance with the Paperwork Reduction Act (PRA) and for submitting USAID's System of Records Notices (SORNs) to the Federal Register and the Office of Management and Budget (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)** provides assistance with posting privacy policies on all USAID Web sites, providing alerts to **www.usaid.gov**, explaining that visitors are being directed to a non-government Web site, and branding and marking the USAID presence on third-party Web sites.

**k.** The **Office of the General Counsel (GC)** interprets privacy statutes, regulations, and other legal authorities; and reviews for legal sufficiency reports, SORNs, proposed rules, and other related matters that USAID publishes in the Federal Register, posts on **www.usaid.gov**, 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. The OIG is responsible for administering the Freedom of Information Act (FOIA) and the Privacy

Act with respect to its own records. For more information about the FOIA, see **ADS 507, Freedom of Information Act**.

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

**n. Contracting Officers** ensure that USAID contracts have the appropriate information privacy clauses sufficient to ensure contractor compliance with federal privacy authorities and protection of the PII under the contract, such as PII collected, used, maintained, and disseminated by USAID or its partner (see **ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology**).

**o.** Agreement Officers must consult with GC to ensure that USAID interagency agreement documents have the appropriate information privacy requirements sufficient to ensure Agency service provider compliance with federal privacy authorities and protection of the PII under the agreement, such as the PII collected, used, maintained, and disseminated by USAID or its partner.

**p. Program Managers (PMs)** are the government officials responsible and accountable for the conduct of a specific government program. PMs are responsible for ensuring the appropriate collection, use, maintenance, and dissemination of that program's PII and for promoting program compliance with federal privacy authorities.

**q. System Owners (SOs)** are organizational officials responsible and accountable for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. An SO:

- Is responsible for the daily program and operational management of a specific USAID information system.
- Ensures privacy documentation is accurate and up-to-date and privacy controls and continuous monitoring of the controls per **NIST 800-53** are implemented for the IT system.
- Prepares and implements a security plan, and monitors its effectiveness (see **ADS 545, Information Systems Security** and section **508.6** of this ADS chapter).
- Protects the privacy and security of PII that an information system collects, uses, maintains, or disseminates, and ensures the system complies with federal privacy authorities.

- Incorporates privacy into the **USAID System Development Life Cycle (SDLC)** to include all mandatory privacy risk and compliance documentation.

- Must be a Direct-Hire (see **ADS 508, Privacy Program, Section 508.2.m. Primary Responsibilities, System Owners** and **ADS 545, Information Systems Security, Section 545.2.j**).

**r.** **System of Records Managers** are government officials responsible and accountable for the conduct of government programs and ensure that the privacy and security of the PII that their Privacy Act Systems of Records collect, use, maintain, disseminate, 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 created by the contracts or agreements they manage that contain PII and 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 to the CISO and Information SO for ensuring the appropriate operational security posture is maintained for their IT systems or programs. They also ensure the security of the PII that their IT systems or programs collect, use, maintain, disseminate, and compliance with federal privacy authorities.

**u.** **USAID Supervisors** are responsible for ensuring that staff 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 take required steps 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 from unauthorized exposure the PII entrusted to their care, to complete privacy compliance activities, to report PII incidents and breaches of PII, and to reduce the volume and types of PII to only that needed for program functions. Members of the workforce are required to successfully complete annual cybersecurity, privacy, 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. In USAID, the AO is the Chief Information Officer.

**x.** The **USAID Privacy Council** is a subcommittee of the Management Operations Council (MOC). Comprised of members from USAID Bureaus and Independent Offices and chaired by the Agency's CPO, the USAID Privacy Council supports the Senior

Agency Official for Privacy (SAOP) and Chief Privacy Officer (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**). Support includes oversight for the Agency's privacy policies and practices and management of privacy risks. The Privacy Council 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 implementation of USAID's cybersecurity risk management measures (OMB Memorandum 17-25). These responsibilities include ensuring that cybersecurity risk management processes align with strategic, operational, and budgetary planning processes in accordance with chapter 35, subchapter II, of title 44, United States Code (USC). The SAORM works closely with the Agency's Executive Management Council on Risk and Internal Control (EMCRIC).

**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; as well as providing 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 (PII)

Effective Date: 04/10/2019

Per OMB A-130 (revised), Personally Identifiable Information (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".

Members of the USAID workforce must protect their own PII and others' PII from being compromised through inadvertent or purposeful disclosure. 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. To determine whether information is PII, the Agency must perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In 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.

PII examples include name, address, social security number (SSN) or other identifying number or code, mother's maiden name, date of birth, place of birth, driver's license

number, medical records 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.

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.

**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, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. A Privacy Act record fits within the definition of PII.

### 508.3.2 Privacy Framework
Effective Date: 04/10/2019

This section explains the framework for the policies and activities of the USAID Privacy Program. The privacy team updates all Privacy Program plans, policies, and procedures as required.

#### 508.3.2.1 Fair Information Practice Principles
Effective Date: 04/10/2019

It is USAID policy to use the Fair Information Practice Principles (FIPPs) as the foundation of the **Privacy Act**, **the E-Government Act Section 208**, and the Office of Management and Budget (OMB) privacy policies applicable to all federal agency information systems and organizations. The FIPPs frame the privacy risks and the 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 specifically the authority that permits the collection of PII and articulate specifically 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 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.

**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-approved record retention schedule.

**e.** Individual Participation and Redress. Involve the individual in the decision-making process regarding the collection and use of his or her PII and seek individual consent for the collection, use, maintenance, and dissemination of PII; and provide a mechanism for appropriate access 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 Privacy Controls

Effective Date: 04/10/2019

The USAID Privacy Program uses the Privacy Impact Analysis (PIA) to evaluate the application of required privacy controls in Agency systems. USAID privacy controls are based on the FIPPs and the guidance provided by the National Institute for Standards and Technology (NIST) in **Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, Rev. 4, Appendix J: Privacy Control Catalog (April 2013)**. The Appendix J Privacy Control Catalog provides a comprehensive framework for privacy policy and implementation by providing a structured set of privacy controls based on best practices that will help USAID and the Privacy Program comply with federal privacy authorities.

The Appendix J Privacy Control Catalog establishes a relationship between privacy and security controls for the purposes of enforcing privacy and security requirements within the NIST Risk Management Framework. Privacy controls from the Privacy Control Catalog are listed in the following table.

| ID | Privacy Controls |
|---|---|
| AP<br>Authority and Purpose | Ensures that USAID identifies the legal bases that authorize a particular PII collection or activity; and specifies in its notices the purposes for which PII is collected. |
| AP-1 | Authority to Collect |
| AP-2 | Purpose Specification |
| AR<br>Accountability, Audit, and Risk Management | Enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that USAID is complying with applicable privacy protection requirements and minimizing overall privacy risk. |
| AR-1 | Governance and Privacy Program |
| AR-2 | Privacy Impact and Risk Assessment |
| AR-3 | Privacy Requirements for Contractors and Service Providers |
| AR-4 | Privacy Monitoring and Auditing |
| AR-5 | Privacy Awareness and Training |
| AR-6 | Privacy Reporting |
| AR-7 | Privacy-Enhanced System Design and Development |
| AR-8 | Accounting of Disclosures |
| DI<br>Data Quality and Integrity | Enhances public confidence that any PII collected and maintained by USAID is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices. |
| DI-1 | Data Quality |
| DI-2 | Data Integrity and Data Integrity Board |
| DM<br>Data Minimization and Retention | Helps USAID to implement the data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. USAID retains PII for only as long as necessary to fulfill the purposes specified in public notices and in accordance with a National Archives and Records Administration-approved record retention schedule. |
| DM-1 | Minimization of Personally Identifiable Information |

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

| ID | Privacy Controls |
|---|---|
| DM-2 | Data Retention and Disposal |
| DM-3 | Minimization of PII Used in Testing, Training, and Research |
| IP<br>Individual Participation and Redress | Addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in USAID decisions made based on the PII. |
| IP-1 | Consent |
| IP-2 | Individual Access |
| IP-3 | Redress |
| IP-4 | Complaint Management |
| SE<br>Security | Supplements the security controls in Appendix F to ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by USAID against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework. |
| SE-1 | Inventory of Personally Identifiable Information |
| SE-2 | Privacy Incident Response |
| TR<br>Transparency | Ensures that USAID provides public notice of its information practices and the privacy impact of its programs and activities. |
| TR-1 | Privacy Notice |
| TR-2 | System of Records Notices and Privacy Act Statements |
| TR-3 | Dissemination of Privacy Program Information |
| UL<br>Use Limitation | Ensures that USAID only uses PII either as specified in its public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly. |

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

| ID | Privacy Controls |
|---|---|
| UL-1 | Internal Use |
| UL-2 | Information Sharing with Third Parties |

### 508.3.2.3 Risk Management Framework
Effective Date: 04/10/2019

The USAID Risk Management Framework (RMF) governs the Agency's federal information systems and includes information privacy functions as required by the **Risk Management Framework for Information Systems and Organizations: A Security Lifecycle Approach for Security and Privacy, NIST SP 800-37, Rev. 2 (September 2017)**. The RMF 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 Life Cycle (SDLC).

### 508.3.2.4 Workforce Use of USAID Information Systems (No Expectation of Privacy)
Effective Date: 04/10/2019

USAID alerts users of the USAID network and systems with a warning banner 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 (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. The user may not rely on any statements or informal policies purporting to provide him/her with any expectation of privacy regarding communications on this system, whether oral or written, by the user's supervisor or any other official, except the USAID CIO.

### 508.3.3 Privacy Rules of Behavior (ROB)
Effective Date: 03/07/2014

This section addresses USAID's Rules of Behavior for the protection of PII.

### 508.3.3.1 Rules of Behavior for Users

Effective Date: 04/10/2019

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:

- Reduce the volume and types of PII they collect for program functions.
- Protect any PII that they handle, process, compile, maintain, store, transmit, or report on in their daily work.
- To protect PII, members of the workforce must:
  - **a.** Use proper collection, storage, transportation, transmission, and disposal methods;
  - **b.** Must not access PII beyond what they need to complete their job duties; and;
  - **c.** Must not disclose PII to unauthorized parties.

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

- Label documents containing PII with the SBU header and footer and use the green SBU Cover Sheet (**AID 568-3**) with paper documents; and
- 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, 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 now 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 (Pub. L. 114-113, Division N)** and November 21, 2016, 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 the possession of USAID and

preventing its breach are necessary to ensure that USAID retains the trust of the American public.

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

All members of the workforce must immediately report all potential and actual privacy breaches or incidents to both the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** and the Privacy team at **privacy@usaid.gov**, regardless of the format of the PII (oral, paper, or electronic) or the manner in which the incidents might have occurred.

For questions about the privacy protection responsibilities of employees, please contact the Privacy Program at **privacy@usaid.gov**. For information on employee responsibilities for classified information, see **ADS 552, Cyber Security for National Security Information (NSI) Systems**, and **ADS 561, Security Responsibilities**.

#### 508.3.3.2 IT Rules of Behavior for Managers

Effective Date: 04/10/2019

This section addresses USAID's policy requirements for the behavior of Agency Program Managers, Systems of Records Managers, System Owners, Information System Security Officers, 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 (i.e., collection, use, retention, processing, disclosure, and destruction) 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 privacy impact assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates 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 must complete a Privacy Threshold Analysis (PTA) at the early program, or system design phase for all new or substantially changed technology, and may be required to complete additional privacy compliance documentation after analysis of the PTA. To be comprehensive and meaningful, PTAs and other privacy compliance documentation require collaboration by program experts as well as experts in the areas of IT, IT security, records management, legal counsel, and privacy.

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 Security Assessment & Authorization (SA&A) process. This process is an evaluation of an IT system's risk, and risk 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 **NIST SP 800-53, Rev. 4**, Appendix J Privacy Controls, SOs must ensure that privacy compliance issues are a part of the SA&A process, which begins with completion of the PTA at the start of the SA&A process. For more information on the SA&A process, see **NIST SP 800-53A, Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans**.

Information System Security Officers (ISSO) must ensure that all appropriate security and privacy controls are applied to their system and must audit and/or monitor the system security and privacy controls to ensure that the safeguards they have applied guard against privacy risks.

USAID Supervisors are responsible for ensuring that members of the workforce receive instruction and training on safeguarding PII. Supervisors are responsible for educating their staff on safeguarding PII and taking appropriate steps, which may include disciplinary action, to address violations of agency privacy policies. For more information about a user's responsibilities as a user of USAID PII, see **ADS 545mbd, Rules of Behavior for Users**.

Misuse, whether intentional or unintentional, or failure to comply with the **Rules of Behavior for Users** may result in appropriate corrective measures in accordance with **ADS 485, Disciplinary Action - Foreign Service** and **ADS 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct - Civil Service**.

In the case of contractor personnel, appropriate measures will be taken by the CO in accordance with the terms and conditions of the award.

### 508.3.4 Accountability, Audit, and Risk Management

Effective Date: 04/10/2019

This section addresses the policy requirements for Accounting, Audit, and Risk Management functions. USAID privacy and risk management evaluators must evaluate how information handling practices may affect individual privacy throughout the information "lifecycle" (i.e., collection, use, retention, processing, disclosure, and destruction), and must incorporate privacy protections at each stage of the information lifecycle.

### 508.3.4.1 Contingency and Continuity Planning
Effective Date: 04/10/2019

System Owners are responsible for ensuring that sufficient contingency and continuity plans are documented for their system. Contingency and continuity planning are management policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergency, system failure, or disaster.

Alternate storage and operations sites used for contingency and continuity purposes must offer the same level of information privacy and security safeguards as the primary sites.

For more information about information security contingency and continuity planning, see the **ADS 545, Information Systems Security,** section on contingency planning and **ADS 545mai, Business Continuity Planning Procedures and Guidelines**. See **ADS 511, Essential Records Program**, for information on identifying and protecting vital records, which are records that specify how USAID and its offices will operate in case of an emergency and those records essential to the continued operation of USAID.

### 508.3.4.2 Privacy Threshold Analysis
Effective Date: 04/10/2019

This section addresses USAID's policy requirements for the creation and maintenance of Privacy Threshold Analysis (PTAs). The privacy team uses a PTA to determine whether any privacy risk exists. The PTA (1) determines whether a particular program will encounter any privacy risks as it performs its functions; and (2) identifies 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 privacy issues involved with systems collecting, using, maintaining, and disseminating PII; systems of records; notice to the public; cloud computing services; third-party Web sites and applications; government contracts; information sharing agreements; information collection via surveys and forms; public Web sites; and new technologies.

Program Managers responsible for IT Systems and System Owners must complete PTAs using the USAID PTA Template before developing a new program information process, and thereafter either before making a significant change to a program information process, when the system undergoes a security authorization, or within three years after the most recent PTA. As long as no additional privacy concerns are identified by the privacy team, the approved PTA will serve as the PIA. The PTA Template contains guidance on how to complete a PTA. For more information about PTAs, see the **PTA Template here**.

If a program will collect PII, then a PIA is required.

### 508.3.4.3 Privacy Impact Assessments
Effective Date: 04/10/2019

This section addresses USAID's policy requirements for the creation and maintenance of Privacy Impact Assessments (PIAs) as required by **Section 208 of the E-Government Act of 2002** and OMB implementing guidance. USAID B/IO/Ms in coordination with the privacy team are responsible for ensuring that technologies developed and used by the Agency sustain and do not erode privacy protections. The PIA is a vital tool that evaluates possible privacy risks and the mitigation of those risks at the beginning and throughout the development life cycle of a program or system.

The privacy team uses the PIA to (1) determine the risks and effects of collecting, using, maintaining, transporting, and disseminating PII; and (2) evaluate protections and alternative processes for handling PII to mitigate potential privacy risks. The length and breadth of a PIA will vary by the size and complexity of the program or system, or the amount and types of PII involved. The PIA helps the Agency determine if adequate privacy protections have been built into the system. Through the PIA and the supporting documentation provided by the system owner, the privacy team determines what privacy controls are required and if they are fully implemented, partially implemented, or non-existent.

USAID must conduct a PIA when:

- Developing or procuring any new technologies or systems that handle or collect PII such as a cloud services, help-desk services, professional services Web sites, tools, mobile applications, and databases.

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

- Updating a system that results in new privacy risks.

- Issuing a new or updated rulemaking that entails the collection of PII.

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

Program Managers, System Owners, and Information System Security Officers must conduct PIAs using the PIA Template before developing a new system and thereafter either; before making a significant change to a system or when the system undergoes a security authorization and the new PTA shows additional privacy risks or within three years after the most recent PIA. A PIA conducted by another federal agency does not fulfill this PIA requirement, even when such an agency is providing computing services for USAID. The PIA Template contains guidance on how to conduct a PIA. For more information about PIAs, see the **PIA Template**.

USAID System Owners must update PIAs to reflect changed information collection authorities, business processes or other factors affecting the PII. In addition, the USAID

Privacy Program must conduct and update PIAs where a significant system change creates new privacy risks. Such significant changes include:

**a.** Conversions - When converting from paper-based records to electronic systems;

**b.** Anonymous to Non-Anonymous - When functions applied to existing information collection change anonymous information into information in identifiable form;

**c.** 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;

**d.** Significant Merging - When agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;

**e.** 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;

**f.** Commercial Sources - When agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources;

**g.** 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;

**h.** 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

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

In addition, pursuant to the guidelines in **OMB M-10-23**, USAID must conduct a PIA when it, or one of its contractors on the Agency's behalf, uses a third-party Web site or application to engage with the public. In general, a USAID program should conduct a single, separate PIA for each third-party Web site or application. For more information on third-party Web sites, see **ADS 545.3.21.1 Third-Party Web Sites** and the Project

Web Site Approval Procedures at **https://pages.usaid.gov/LPA/website-governance-board-approval-procedures** (this link is only accessible to USAID.gov users).

PIAs provide information on how USAID programs handle PII so that the American public has assurances that their government is protecting their PII. The PIA is a risk-based analysis that enables USAID to determine the level of privacy risk acceptable to the systems that support the conduct of USAID business functions. Risk mitigation helps USAID to (1) cost-effectively reduce privacy risks to an acceptable level; (2) address privacy throughout the lifecycle of each system; and (3) ensure compliance with the federal authorities and USAID policies, procedures, and standards. The PIA's privacy risk mitigation function works hand-in-hand with USAID's Security Assessment & Authorization (SA&A), Security Controls Assessments (SCA), Risk Assessment, and Plan of Action and Milestones (POA&M) processes.

### 508.3.5 Establishing Authority and Purpose to Collect PII

Effective Date: 04/10/2019

USAID uses the PII Inventory, Privacy Impact Assessment (PIA), Privacy Act Section (e)(3) Statement (Privacy Act Statement), and System of Records Notice (SORN) processes to identify the legal bases that authorize PII collection or activity that impacts privacy. USAID then uses PIAs, Privacy Act Statements, and SORNs to provide notice of the purposes for which PII is collected.

#### 508.3.5.1 Privacy Review of Software and Hardware for Agency Use

Effective Date: 04/10/2019

If a B/IO/M needs software or hardware that is not on the **M/CIO Approved Software** or **IT Standards list**, the B/IO/M must submit a **software and hardware approval request (SHARP)** to M/CIO for consideration. The Privacy Team must determine if PII data is properly secured, at rest and in transit, by the proposed software or hardware solution. The B/IO/M must request approval by submitting a software and hardware approval request (SHARP). See the How to Enter a Software and Hardware Approval Request (**https://usaiditsm.service-now.com/nav_to.do?uri=%2Fkb_view.do%3Fsysparm_article%3DKB0011369**). B/IO/Ms are prohibited from purchasing equipment that is not approved by M/CIO. See **ADS 547** for additional guidance on the SHARP.

#### 508.3.5.2 Privacy Considerations for Contracts

Effective Date: 04/10/2019

Pursuant to the **Privacy Act of 1974** Section(m)(1), Operating Units (OU) must advise Contracting Officers when supplies/services under a procurement request involves 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 System Owners must coordinate with the CO to ensure that contracts include appropriate terms and conditions ensuring

contractor compliance with the Privacy Act and the federal authorities that flow from it, including the **E-Government Act Section 208**.

In addition to 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 are provided at **Acquisition & Assistance Policy Directive (AAPD) 16-02 (Revised)** and **ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology.** The AAPD 16-02 (Revised) and 302mah provides requirements for information technology security 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 that all required privacy training (onboarding and annual) is completed by contractor employees. USAID provides the initial privacy training, and annual privacy training thereafter, to contractor (and subcontractor) employees for the duration of all USAID contracts. The FAR states that a contractor employee must not have access to a system of records or handle personally identifiable information until the employee has completed training. CORs are responsible for ensuring that contractors 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 the contractor is aware that they need to set up an account with USAID University at **https://pages.usaid.gov/HCTM/usaid-university** and complete the mandatory USAID privacy training annually (see **508.3.5.9**).

In addition, all Agency Contracting Officers must work with Program Managers, System of Records Managers, and System Owners to incorporate the privacy protections in USAID IT Security contract clauses.

For more information on information technology resources contracting and contracting generally, see **ADS 302, USAID Direct Contracting** and **ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology.**

### 508.3.5.3 Privacy Considerations for Interagency Agreements

Effective Date: 04/10/2019

Pursuant to the **Privacy Act** Section(m)(1), USAID Agreement Officers must work with Program Managers, System of Records Managers, and System Owners to include in interagency agreements appropriate privacy protection language in order to ensure Participating or Servicing Agency compliance with the Privacy Act and the federal authorities that flow from it, including the **E-Government Act Section 208**.

The USAID Agreement Officer (whether a warranted contracting officer or an Assistant Administrator), as the signatory for an interagency agreement, bears the legal responsibility for the agreement. The Agreement Officer must provide overall liaison and coordination with the Participating or Servicing Agency on interagency agreements that

the Agreement Officer signs. For more information about Agreement Officers, see **ADS 103, Delegations of Authority**, and **ADS 306, Interagency Agreements**.

In addition, USAID Agreement Officers must work with General Counsel, PMs, System of Records Managers, and SOs to incorporate the following privacy protections in interagency agreements:

**a.** USAID control of PII in systems for the length of the interagency agreement and beyond;

**b.** Participating or Servicing Agency has no ownership of the PII;

**c.** Participating or Servicing Agency has no access or retention rights to the PII beyond those authorized by the interagency agreement and only during the life of the interagency agreement;

**d.** Participating or Servicing Agency must provide USAID access to PII when needed; and

**e.** Describe the responsibilities and liabilities of the Participating or Servicing Agency and for USAID for PII incidents and breach response activities.

For more information on agreements, see **ADS 306, Interagency Agreements**.

#### 508.3.5.4 Privacy Considerations for Cloud Computing Services

Effective Date: 04/10/2019

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 collect, use, maintain, or disseminate PII without prior approval from the Office of the Chief Information Officer (M/CIO) (see **software and hardware approval request (SHARP)** for additional guidance).

Agency Contracting Officers and Contracting Officer Representatives must work with General Counsel, Program Managers, System of Records Managers, and System Owners to include in terms of service and contracts appropriate privacy protection language (see **ADS 545** and **ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology**) to:

**a.** 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 558 for guidance on social media channels); and

**b.** 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 U.S., and location changes may require amendment of privacy compliance documentation such as PIAs and SORNs.

How a cloud services provider addresses privacy concerns within their environment may affect the overall price and technical structure for a proposed cloud computing solution. B/IO/Ms must work with the privacy team to identify privacy requirements as early as possible in the information lifecycle to understand fully 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**.

### 508.3.5.5 Incorporating Privacy into the Information Lifecycle

Effective Date: 04/10/2019

OMB has directed all federal agencies, including USAID, to incorporate privacy analyses into each stage of the information lifecycle (i.e., collection, use, retention, processing, disclosure, and destruction), from the early design stage to start up, use, and ultimate disposal. The Privacy Program strives to implement substantive privacy protections such as notice and consent, limitations on data collection and retention, and data accuracy, as well as procedural safeguards, aimed at integrating the Fair Information Practice Principles (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 information lifecycle management, especially at the critical initiation phase. As information and devices become increasingly mobile and the amount of PII collected increases, it is 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.

In that light, USAID is incorporating privacy compliance requirements into its Security Assessment & Authorization (SA&A) process, which is an evaluation of an IT system risk and risk mitigating controls. The SA&A process takes into account specific security requirements, verifies the existence of security controls, and summarizes residual risk.

Privacy compliance issues will become part of the SA&A process starting with the Privacy Threshold Analysis (PTA).

### 508.3.5.6 Privacy Awareness Training

Effective Date: 04/10/2019

M/CIO/IA must provide annual privacy awareness training to all USAID employees and contractors available online through USAID University. This annual training provides the USAID workforce with a better understanding of the basic knowledge necessary for protecting PII data elements in accordance with USAID and Privacy Act requirements. Workforce members who do not complete annual privacy awareness training by the deadline will have their access to the USAID network suspended by the Chief Privacy Officer (CPO).

M/CIO/IA provides privacy training every other week as part of New Employee Orientation (NEO) and, on alternate weeks, as part of non-NEO Contractor On-Boarding training. (Note: Attending NEO/non-NEO privacy training does not exempt employees from completing the online annual privacy awareness training.)

In addition, M/CIO/IA provides targeted, role-based training a minimum of once annually to those members of the workforce having responsibility for PII or for activities that involve PII. Direct-Hire Supervisors may request additional role-based privacy training by emailing **privacy@usaid.gov**.

M/CIO/IA must ensure that members of the workforce certify acceptance of responsibilities for privacy requirements at a minimum annually by completing the annual cybersecurity training and sign a copy of the ROB prior to getting access to a system user account or data. For more information about IT Security Training and Rules of Behavior for Users, see the **ADS 545, Information Systems Security,** sections on Rules of Behavior (ROB) and Information Security Awareness, Training, and Education, and see **ADS 545mbd, Rules of Behavior for Users**.

### 508.3.5.7 Privacy Reporting

Effective Date: 03/07/2014

The USAID Senior Agency Official for Privacy (SAOP) reports to OMB on an annual basis according to the requirements of FISMA. The USAID SAOP reports include statistics on outstanding and completed PIAs and SORNs for USAID systems, as well as other data requested by OMB.

The criteria for identifying PII and for conducting PIAs and SORNS are based on statutory thresholds in the Privacy Act and Section 208 of the E-Government Act and on OMB guidance. The same criteria apply to reporting systems to OMB; that is, when USAID conducts a PIA or creates a SORN, it must report it to OMB under FISMA.

For more information on identifying what data is PII, see section **508.3.1, Personally Identifiable Information (PII)**. For more information on the threshold for conducting

PIAs, see section **508.3.5.4, Privacy Impact Assessments**. For more information on the threshold for creating SORNs, see section **508.3.10.2, System of Records Notices**.

The SAOP also responds to congressional inquiries on an ad hoc basis.

### 508.3.5.8 Automating Privacy Controls
Effective Date: 03/07/2014

USAID is employing technologies and system capabilities to automate privacy controls on the collection, use, retention, and disclosure of PII. By building privacy controls into system design and development, USAID mitigates privacy risks to PII, thereby reducing the likelihood of PII breaches and other privacy-related incidents. USAID regularly monitors system use and the sharing of PII to ensure that the use/sharing 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.

### 508.3.6 Data Quality and Integrity
Effective Date: 04/10/2019

System Owners and/or members of the workforce collecting data must take reasonable steps to protect the quality, timeliness, relevance, and integrity of the PII that it collects, uses, maintains, and disseminates. All employees are responsible for using PII properly. This includes maintaining the quality and integrity of PII collected, used, maintained, and disseminated by USAID. For more information about data quality, see **ADS 578, Information Quality Guidelines**, and **ADS 597sad, Data Quality Assessment Checklist**.

Program Managers, System of Records Managers, and System Owners must validate PII that is obtained from sources other than the subject individuals or the authorized representatives of such individuals. This is necessary to assure fairness in any determination about an individual and promotes the Fair Information Practice Principle of Data Quality and Integrity.

USAID System Owners must implement security and privacy controls to maintain the accuracy and consistency of PII throughout the information lifecycle. This is necessary to assure fairness in any determination about an individual and promote the Fair Information Practice Principles.

If USAID participates in or conducts matching programs, a USAID Data Integrity Board must review, approve, and maintain all written agreements for receipt or disclosure of USAID records for matching programs. This assures compliance with all relevant statutes, regulations, and guidelines. For more information on data integrity boards, see **5 USC 552a(u)**.

### 508.3.7 Matching Programs and Agreements
Effective Date: 04/10/2019

USAID may participate in multiple matching programs, which are computerized comparisons of two or more automated systems of records. 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. Employees 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 **508.11.2, Sharing Information with Third Parties**).

### 508.3.8 Data Minimization and Retention
Effective Date: 04/10/2019

Members of the USAID workforce must only collect, use, and retain PII that is relevant and necessary for the purpose for which it was originally collected, and retain PII only as long as necessary to fulfill the purposes specified in public notices and in accordance with a National Archives and Records Administration-approved record retention schedule. For more information about records management, see **ADS 502, The USAID Records Management Program**.

All workforce members must use PII properly and must reduce (to the minimum necessary for proper performance of their program purposes) their use of PII, as well as the volume and types of PII they collect. Members of the workforce must also retain PII only as long as necessary to accomplish their program purposes.

#### 508.3.8.1 PII Review and Reduction
Effective Date: 04/10/2019

Under OMB guidance in Memorandum **M-07-16**, USAID must reduce its PII collection and holdings to the minimum necessary to accomplish its mission. By reducing PII, USAID is actively taking steps to reduce the risk associated with a privacy breach. USAID put forth a PII Reduction Plan that details the privacy team's process to identify, review, and make recommendations to reduce PII holdings within USAID's information systems. The plan includes an initial evaluation of PII holdings and establishes a schedule for reviewing those holdings at least annually to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose (see USAID Social Security Number Collection and Use Policy (accessible via the USAID intranet only) at: https://pages.usaid.gov/sites/default/files/social_security_number_collection_and_use_policy.pdf).

### 508.3.8.2 Social Security Number Use Reduction and Elimination

Effective Date: 03/07/2014

Because of the elevated risk of harm to individuals from the compromise of Social Security Numbers (SSNs), the privacy team focuses especially on the reduction and elimination of the USAID dependence on 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 team has developed a plan to review the use of SSNs and to reduce USAID reliance on SSNs, which reduces the risk to individuals of having their identity compromised if there is a privacy breach involving SSNs. The privacy team works with Forms Owners, System of Records Managers, and System Owners to reduce the volume of SSNs collected and retained to the minimum necessary to accomplish a business function, and to limit the number of employees who have access to SSNs to only those with a need to know in order to complete their job functions. For more information on SSN use reduction and elimination, see **OMB Memorandum M-17-12**.

### 508.3.8.3 Restriction on Mailing Documents Containing Social Security Numbers and PII

Effective Date: 04/10/2019

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 the 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 are mailed to posts abroad that contain SSN or PII should 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 utilized, 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 partial redaction of the SSN or PII), please contact the Agency's privacy team at

**privacy@usaid.gov**. Please contact the Bureau's Office of Management Services (M/MS) for guidance on mailing materials at **facilities@usaid.gov**.

#### 508.3.8.4 PII Retention and Disposal
Effective Date: 04/10/2019

All members of the workforce must carefully store and destroy PII and media containing PII by USAID-approved methods. Members of the workforce must secure PII in documents or on media within a locked office or suite, or secured in a locked container such as a 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, Section 545.3.11.6, Media Sanitization (MP-6)**, 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 Disposition Schedules and USAID-approved disposition schedules (see **ADS Chapter 502, The USAID Records Management Program**.)

#### 508.3.8.5 PII Use for System Testing, Training, and Research
Effective Date: 04/10/2019

The use of PII in testing, training, and research increases the risks of unauthorized disclosure or misuse of such PII. System Owners and Program Managers are not authorized to use real PII during system testing, training, or research and must take measures to eliminate PII from data used for such purposes. If PII must be used for system testing, training, or research, SOs and PMs must conduct a PIA before using the PII for system testing, training, or research; must protect PII at the same level that it is protected in the production environment; and must minimize any associated risks and restrict the use, amount, and types of PII for these purposes. For more information on protecting PII during system testing, training, and research, see **NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**.

### 508.3.9 Individual Participation and Redress
Effective Date: 07/30/2019

This section addresses the policy requirements for individual participation, redress, and complaint management. Participation includes consent and access to PII by the subject individual, and 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. The OIG is responsible for administering the FOIA and the Privacy Act with respect to its own records.

#### 508.3.9.1 Individual Redress
Effective Date: 04/10/2019

**The Freedom of Information Act (FOIA)** provides that any person has a right, enforceable in court, to obtain access to federal agency records, except such records (or portions of them) protected from public disclosure.

**The Privacy Act** provides an individual three primary rights: (1) to access records about oneself, subject to the Privacy Act's exemptions; (2) to amend a nonexempt record if it is inaccurate, irrelevant, untimely, or incomplete; and (3) to file suit against the Federal Government to access or amend its records, or for violations of the Privacy Act.

**The Privacy Act** provides individuals with a means to seek access to and amendment of their records, but the **Privacy Act** pertains only to records about individuals who are either U.S. citizens or lawfully admitted permanent resident aliens. The FOIA, on the other hand, covers virtually all agency records under the in the possession and control of a federal executive branch agency. If the records sought are about an individual, that individual can request them under both **FOIA** and the **Privacy Act**.

The Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD) is responsible for managing and responding to FOIA requests and 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**. For more information on FOIA issues and requests, see **FOIA requests** and **ADS 507, Freedom of Information Act**.

### 508.3.9.2 Complaint Management
Effective Date: 04/10/2019

The privacy team 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 team investigates privacy complaints pursuant to the **Privacy Act of 1974** and the **Freedom of Information Act** related to records about individuals (U.S. citizens and lawfully admitted permanent resident aliens).

### 508.3.10 Security
Effective Date: 04/10/2019

This section addresses the policy requirements for security functions specific to PII. The privacy team requires security controls to protect PII. Such security controls include identifying and reducing the use of PII and planning for, and responding to, privacy incidents.

### 508.3.10.1 Inventory of Personally Identifiable Information
Effective Date: 04/10/2019

The USAID Privacy Program must review its PII holdings at a minimum annually and ensure, to the maximum extent practicable, 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 maintains an inventory that contains a listing of all information systems, information collection forms, and systems of records identified as involving the collection, use, maintenance, or dissemination of PII. The privacy team uses this baseline PII inventory to evaluate USAID collection, use, maintenance, and dissemination of PII and to identify areas where USAID can reduce or eliminate its dependence on PII.

### 508.3.10.2 Security Controls for Personally Identifiable Information

Effective Date: 03/07/2014

PII is a type of Sensitive But Unclassified (SBU) information. Because it is SBU information, PII requires greater controls against unauthorized access and disclosure than other information that is Unclassified. Employees must label documents containing PII with the SBU header and footer and use the green SBU cover sheet with paper documents. Employees must 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 are given access.

FISMA requires each agency to implement a comprehensive security program to protect the agency's information and information systems. System Owners and Information System Security Officers, in coordination with the USAID Information Assurance Office (M/CIO/IA), must implement the catalog of security and privacy controls in **NIST SP 800-53, Rev. 4**, which provides a range of safeguards and countermeasures for USAID information and information systems. The System Owners and Information System Security Officers apply security and privacy controls to protect against the loss, unauthorized access, or unauthorized disclosure of PII.

### 508.3.10.3 Encrypting PII

Effective Date: 04/10/2019

Under various OMB Memoranda and Security Controls in **NIST SP 800-53, Rev. 4**, SOs and ISSOs must ensure that all PII is encrypted at rest, in motion, during remote and wireless access, and on all removable media, such as laptops and Personal Digital Assistants (iPads and iPhones).

Individuals must not email PII from a usaid.gov email address without protecting the PII. This means that 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" or another email domain. In addition, individuals must ensure that PII is encrypted on all removable media, such as CDs, DVDs and thumb drives. For more information about encrypting PII, see **ADS 545, Information Systems Security,** section on Protecting Privacy Sensitive Systems and **ADS 545mbd, Rules of Behavior for Users**. Review more details about encryption in section **508.3.3.1, Rules of Behavior for Users**. Additionally, see the November 21, 2016, Agency Notice, "**Mandatory Encryption of Email Attachments Containing PII**".

### 508.3.10.4 Remote Access to PII
Effective Date: 04/10/2019

When working remotely, individuals must use a USAID-issued electronic device or an RSA-token-enabled Citrix connection (**remoteaccess.usaid.gov**) when they collect, use, maintain, and disseminate PII. For more information about remote access requirements, see **ADS 545, Information Systems Security**, section **545.3.2.11, Remote Access (AC-17)**, and **ADS 549, Telecommunications Management**, section **549.3.5.1, Remote Access** (see also **ADS 405, Telework**, section **405.3.9, Security and Safeguarding of Government Information**).

### 508.3.10.5 Access to Electronic Records of Former Employees
Effective Date: 04/10/2019

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

### 508.3.10.6 Privacy Breach Reporting and Response
Effective Date: 04/10/2019

USAID must manage, in accordance with federal laws and regulations, the information it collects, uses, maintains, and disseminates in support of its mission and business functions. 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 experienced by the individual. Although most incidents involve information technology, a privacy breach may also involve physical security considerations (such as paper documents, removable media, and mobile devices). Certain suspected and or confirmed breaches must be reported by USAID CSIRT to the United States Computer Emergency Readiness Team (US-CERT), as instructed by the Department of Homeland Security and Office of Management and Budget. All personnel operating on behalf of USAID must report immediately upon suspicion or discovery of any incident that may be a potential privacy breach to the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** and the Privacy team at **privacy@usaid.gov**, regardless of the format of the PII compromised (oral, paper, or electronic) or the manner in which the incidents might have occurred. The USAID Privacy Incident Response Team (PIRT) within the Privacy team evaluates the incident. If the PIRT determines that USAID should report the incident to US-CERT, the privacy team submits a report to the USAID Computer Security Incident Response Team (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 U.S.-CERT within one hour of discovery.

Depending on the level and suspected impact of the breach, the PIRT will notify the Breach Response Team (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 the group of agency officials designated by the head of the agency that the SAOP may convene to respond to a breach. The Breach Response Team is responsible for advising the head of the agency on effectively and efficiently responding to a breach. Decisions and recommendations are made by consensus. In addition, the Breach Response Team members must participate in the tabletop exercise held annually.

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

- The SAOP;
- Chief Privacy Officer;
- The Chief Information Officer (CIO) or the Deputy Chief Information Officer;
- The Chief Information Security Officer (CISO), also known as Senior Agency Information Security Officer (SAISO);
- General Counsel;
- Bureau for Legislative and Public Affairs; and
- The Responsible Office (who owns the system).

**OMB Memorandum M-17-12** defines the following terms:

Incident: An occurrence that 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 personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

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 misplaced or lost paper files, etc.

### 508.3.11 Transparency
Effective Date: 04/10/2019

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 Web sites and paper forms and surveys, as well as posting Web site privacy policies, **PIA summaries**, and SORNs on USAID public Web sites.

#### 508.3.11.1 Privacy Act Section (e)(3) Statements or Notices
Effective Date: 04/10/2019

All forms, both paper and electronic, collecting information under the Privacy Act for a "System of Records" must place a Privacy Act (e)(3) Statement on the form, which is used to collect the information or on a separate form that can be retained by the individual.

Per the **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.

The notice must be located and accessible on the form or survey where the PII is collected, whether on a Web site, electronic media, or paper. A Privacy Act Statement must be included on all USAID forms and surveys (both internal and external) that collect PII on individuals (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 **ADS 508mag, Guidance for USAID Privacy Act Section (e)(3) Statements or Notices Template**.

#### 508.3.11.2 Systems of Records Notices
Effective Date: 04/10/2019

This section addresses the policy requirements for Systems of Records Notices under the **Privacy Act of 1974**. USAID must conform to the notice requirements of the **Privacy Act**. **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 creates, alters, or deletes a system of records, USAID must create and publish in the Federal Register a notice of the existence and character of the system of records. Program Managers and System of Records Managers must complete such a System of Records Notice (SORN) using the SORN template before collecting PII and thereafter periodically before making changes to the system of records.

There are three types of systems of records: Internal; Government-wide; and Central. Internal systems of records are records created within USAID for its employees or administrative duties or mission and are owned by USAID to cover its internal records. Government-wide systems of records are records for which one central federal agency writes the policy but does not have physical custody as a matter of necessity. Central systems of records are records for which one agency writes the policy and actually has physical custody, but for which other federal agencies are permitted to maintain copies. USAID will use government-wide or central SORNs for the appropriate systems of records when such SORNs specifically state that they cover records held by all federal agencies or specifically USAID.

The SORN template contains guidance on how to conduct the SORN and information on the USAID SORN process requirements. The privacy team uses the information provided to complete the OMB authorization process, notify Congress, and publish the SORN in the Federal Register and then post it on **www.usaid.gov**. For more information about SORNs, see **ADS 508maa, USAID System of Records Notice Template**. **OMB Circular A-108**, “Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act” provides more information on SORNs.

### 508.3.11.3 Privacy Issues with Information Collection Requests

Effective Date: 04/10/2019

This section addresses the policy requirements for the privacy issues related to collections of information regulated under **Paperwork Reduction Act (PRA)**.

The PRA and subsequent regulatory guidance established requirements for information collection requests (ICRs), and for minimizing the paperwork burden for individuals, small businesses, educational, nonprofit institutions, federal contractors, state, local and tribal governments, and other persons from the collection of information by or for the Federal Government. Surveys, questionnaires, registration forms, Web sites, and databases are subject to PRA requirements.

The Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD) is responsible for managing the ICR approval process. Program Managers and System Owners must work with M/MS/IRD to comply with the OMB procedures for ICRs. For more information on the ICR approval process, see **ADS 505, Forms Management Program** and **ADS 506, Reports Management**.

Information collections are subject to all federal privacy compliance requirements, including PTAs, Privacy Act Statements, SORNs, and PIAs. Program Managers, System of Records Managers, System Owners, and Information System Security Officers must complete these privacy compliance documents before a USAID program starts to collect information related to the ICR and then before they make any changes to the program's information collection process. See the specific sections in this ADS chapter for more information: PTAs, PIAs, SORNs, and Privacy Act Statements.

### 508.3.11.4 Public Web Site Privacy Policies

Effective Date: 03/07/2014

USAID's use of publicly facing (external) Web sites creates new challenges for privacy protections while enabling greater dissemination or exchange of information via Internet technologies. How and when USAID collects PII from Web site visitors is not always obvious to the Web site visitor. USAID Web sites are those funded in whole or in part by USAID and operated by USAID, contractors, or other organizations on behalf of USAID.

SOs responsible for USAID public Web sites must post privacy policies that clearly and concisely inform visitors to the Web site what information USAID collects about individuals, why the agency collects the information, and how the agency will use the information. SOs must provide Web site privacy policies that are clearly labeled and easily accessed by visitors to the Web sites, and post privacy policies at major entry points and Web sites where substantial PII is collected.

SOs must monitor their external Web sites to ensure compliance with privacy requirements. The CPO may require corrective actions for sites determined to be non-compliant and may shut down Web sites until the SOs correct the deficiencies. For more information about SO's responsibilities regarding USAID public Web site privacy policies, see **ADS 508mak, USAID Public Web Site Privacy Policies Requirements**, **ADS 557, Public Information**.

### 508.3.11.5 Third-Party Web Sites and Applications

Effective Date: 03/07/2014

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

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

**b.** External Links. System Owner must provide an alert to the visitor explaining that they are being directed to a non-government Web site that may have different privacy policies from those of the Agency's official Web site.

**c.** Embedded Applications. System Owner must take the necessary steps to disclose the third party's involvement when it is embedded in the USAID Web site.

**d.** Agency Branding. System Owner must apply appropriate branding to distinguish USAID activities from those of non-government actors.

**e.** Information Collection. System Owner must ensure that USAID collects only the minimum PII necessary to accomplish a purpose required by statute, regulation, or executive order.

**f.** Privacy Impact Assessments (PIAs). System Owner must conduct an adapted PIA whenever USAID's use of a third-party Web site or application makes PII available to the Agency.

**g.** Agency Privacy Policies. System Owner must ensure that the USAID Web site privacy policy accurately describes their use of third-party Web sites and applications.

**h.** Agency Privacy Notices. To the extent feasible, the System Owner must post a Privacy Notice on the third-party Web site or application itself.

### 508.3.12 Use Limitation

Effective Date: 04/10/2019

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. Employees must follow the Rules of Behavior for Users 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 employees, see **ADS 545mbd, Rules of Behavior for Users**.

#### 508.3.12.1 Internal Use

Effective Date: 04/10/2019

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 in the course of their job responsibilities.

### 508.3.12.2 Open Government and Open Data
Effective Date: 04/10/2019

In compliance with **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 is required to implement tools and processes that will 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, consult **ADS 579, USAID Development Data**.

The Operating Unit that funded the dataset must complete an Open Data Privacy Analysis (ODPA) using the **USAID Open Data Privacy Analysis Template (ODPA)** before the dataset is posted to a public Web site, and thereafter periodically, before updating datasets on Web sites available to the public.

The privacy team 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 Web site available to the public. The CORs and AORs in the program responsible for the dataset must assess whether a particular dataset contains PII and must comply with all privacy protection requirements, such as removing PII from the dataset and sensitive metadata associated with that dataset, before posting the dataset to a Web site available to the public.

For more information on COR responsibilities, see **ADS 302, USAID Direct Contracting**. For more information on AOR responsibilities, see **ADS 303, Grants and Cooperative Agreements to Non-Governmental Organizations**. For more information on USAID's policy on development data, see **ADS 579, USAID Development Data**.

### 508.3.12.3 Sharing PII with Third Parties
Effective Date: 04/10/2019

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 when sharing PII with third parties, B/IO/Ms must enter into a memorandum of understanding (MOU), memorandum of agreement (MOA), letter of intent, computer matching agreement, 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, 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, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy** and **OMB Memorandum M-11-02, Sharing Data While Protecting Privacy**.

### 508.3.12.4 Freedom of Information Act Disclosure Limitations
Effective Date: 03/07/2014

The Freedom of Information Act (FOIA) provides that any person 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. Under the FOIA, agencies must disclose any requested records, except such records (or portions of them) that FOIA exempts protected from public disclosure. The FOIA exemptions provide protection for nine categories of records, including records, the disclosure of which 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)**.

### 508.3.12.5 Privacy Act Disclosure Limitations and Routine Uses
Effective Date: 04/10/2019

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:

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

**b.** Per a Freedom of Information Act (FOIA) request (for more information about FOIA requests, see **ADS 507**); and

**c.** Under a routine use specified in the appropriate SORN.

For the routine uses specified in SORNs, as required by **OMB Circular A-108**, 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.

### 508.3.12.6 Privacy Act Disclosure Exemptions
Effective Date: 04/10/2019

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

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

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

**c.** General Exemptions, **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-130**, the USAID Privacy Program must review each system of records for which an exemption has been promulgated every four years to determine whether such exemption is still needed.

### 508.3.12.7 Civil Remedies and Criminal Penalties for Unlawful Disclosure

Effective Date: 03/07/2014

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**.

### 508.3.13 Data Loss Prevention (DLP)

Effective Date: 04/10/2019

Both federal and USAID policy requires personally identifiable information to be protected from loss, disclosure, or any other unauthorized use. The USAID Privacy Program is responsible for providing the requirements for an Agency Data Loss Prevention (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 USAID Privacy team may provide remedial training to USAID staff and contractors who make isolated and unintentional policy violations. Violations caused by staff negligence, intentional violations, and repeat violations by staff who have already been re-trained, may be referred to the individual's supervisor or Contracting Officer Representative (COR). This allows the supervisor or COR, in consultation with the Privacy team, to determine if additional action, including discipline or remedial training, is appropriate.

The Agency Privacy team must formulate the functional requirements for DLP technologies. The Privacy team will review the implementation of these requirements

annually to 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.

## 508.4 MANDATORY REFERENCES

### 508.4.1 External Mandatory References

#### 508.4.1.1 Statutes and Regulations

Effective Date: 04/10/2019

**a.** 22 CFR 215

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

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

**d.** Confidential Information Protection and Statistical Efficiency Act of 2002, as amended at 44 USC 3501 Note

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

**f.** Consolidated Appropriations Act of 2016 (Cybersecurity Act of 2015 (P.L. 114-113, Division N)

**g.** E-Government Act of 2002, Section 208, as amended at 44 USC 3501 Note

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

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

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

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

**k.** Federal Information Security Management Act of 2002, as amended at 44 USC 3541-3549

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

**m.** Health Information Portability and Accountability Act of 1996, (Pub. L 104-191)

**n.** Paperwork Reduction Act of 1995, as amended at 44 USC 3501-3521

**o.** Privacy Act of 1974, as amended at 5 USC Section 552a

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

### 508.4.1.2 Office of Management and Budget (OMB)

Effective Date: 04/10/2019

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

**c.** OMB Circular A-130, Managing Federal Information as a Strategic Resource

**d.** OMB Circular A-123 Management's Responsibility for Enterprise Risk (July 15, 2016)

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

**f.** OMB Memorandum M-99-05, Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"

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

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

**i.** OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 200

**j.** OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy

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

**l.** OMB Memorandum M-10-06, Open Government Directive

**m.** OMB Memorandum M-10-22, Online Use of Web Measurement and Customization Technologies

**n.** OMB Memorandum M-10-23, Agency Use of Third-Party websites and Applications

**o.** OMB Memorandum, Model Privacy Impact Assessment for Agency Use of Third-Party Web Sites and Applications

**p.** OMB Memorandum M-11-02, Sharing Data While Protecting Privacy

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

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

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

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

**u.** OMB Memorandum M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices

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

#### 508.4.1.3 National Institute of Science and Technology (NIST)

Effective Date: 04/10/2019

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

**b.** NIST SP 800-37, Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security lifecycle Approach

**c.** NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J: Privacy Controls

**d.** NIST SP 800-53A, Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans

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

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

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

### 508.4.1.4 U.S. Department of State
Effective Date: 03/07/2014

**a.** 12 FAM 540, Sensitive But Unclassified Information

### 508.4.2 Internal Mandatory References
Effective Date: 04/10/2019

**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 405, Telework

**g.** ADS 485, Disciplinary Action - Foreign Service

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

**i.** ADS 502, The USAID Records Management Program

**j.** ADS 505, Forms Management Program

**k.** ADS 506, Reports Management

**l.** ADS 507, Freedom of Information Act (FOIA)

**m.** ADS 508maa, USAID System of Records Notice Template

**n.** ADS 508mag, Guidance for USAID Privacy Act Section (e)(3) Statements or Notices

**o.** ADS 508mak, USAID Public Web Site Privacy Policies Requirements

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

**p.** **ADS 516, Federal Register Notices**

**q.** **ADS 545, Information Systems Security**

**r.** **ADS 545mbd, Rules of Behavior for Users**

**s.** **ADS 557, Public Information**

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

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

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

**w.** **ADS 596mab, Management Control Review Committee (MCRC) Charter**

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

**y.** **USAID System Development Lifecycle** (Please note that this link can only be accessed on the USAID network.)

## 508.5 ADDITIONAL HELP

Effective Date: 04/10/2019

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

**b.** **AID 545-9 USAID Information System Owner Letter of Acknowledgement**

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

**d.** **FedRamp Control Specific Contract Clauses**

## 508.6 DEFINITIONS

Effective Date: 04/10/2019

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. (**Chapter 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 such as the Privacy Act or the Freedom of Information Act. (**Chapter 508**)

**Agreement Officer**
A person with the authority to (1) enter into, administer, terminate, and close out assistance agreements, and (2) make related determinations and findings on behalf of USAID. An Agreement Officer may only act within the scope of a duly authorized warrant or other valid delegation of authority. The term "Agreement Officer" includes persons warranted as "Grant Officers." It also includes certain authorized representatives of the Agreement Officer acting within the limits of their authority as delegated by the Agreement Officer. (**Chapters 300, 303, 304, 306, 508, 621**)

**Breach**
The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, or an authorized user for an other than authorized purpose, have access or potential access to personally identifiable information, whether physical or electronic. (**Chapter 508**)

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

**Dataset**
An organized collection of structured data, including data contained in spreadsheets, whether presented in tabular or non-tabular form. For example, 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 (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**
This is 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. Such collections include 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 “personally identifiable information”. (**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.] Source: NIST: Key Glossary of Information Security Terms. (**Chapter 502, 508, 509, 545, 550, 620**)

**Information System Security Officer (ISSO)**
Individual responsible to the senior agency information security officer, AO, or information SO for ensuring the appropriate operational security posture is maintained for an information system or program. (**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 FAA section 632(b), the Economy Act, the Government Management Reform Act 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** and **508**)

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

**Matching Agreement**
The agreement establishing 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 system of records (SOR), 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**)

**Participating Agency**
A federal agency that enters into a Participating Agency Service Agreement (PASA), Resources Support Services Agreement (RSSA), or Participating Agency Program Agreement (PAPA) with USAID under the authority of FAA section 632(b). (**Chapter 306** and **508**)

**Personal Identifier**
A name, number, or symbol that is unique to an individual. Examples are the individual's name and Social Security Number, and may also include fingerprints or voiceprints. (**Chapter 508**)

**Personally Identifiable Information (PII)**
Per OMB A-130 Personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual. (**Chapter 508**)

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

**Privacy Act Notice**
A statement or notice, required by Privacy Act Section (e)(3), appearing on a Web site 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 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 and that contains his 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 or notice, required by Privacy Act Section (e)(3), appearing on a Web site 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. The public or users must be notified 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 Notice. (**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 Threshold Assessment (PTA)**
A Privacy Threshold Assessment or Analysis (PTA) provides a high-level description of an information system including the information it contains and how it is used. The PTA determines and documents whether or not a PIA or SORN is required. (**Chapter 508**, **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. (**Chapter 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 which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act 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. (**Chapter 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**
A significant change is defined as a change that is likely to affect the security state of an information system. Significant changes to an information system may include for example: (1) installation of a new or upgraded operating system, middleware component, or application; (2) modifications to system ports, protocols, or services; (3) 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, the 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**
An employee that is responsible for the "direction" of subordinates within his/her 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**
Refers to any information system or application, and 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 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, which 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 an individual can be notified at his request if the system of records contains a record pertaining to him; (8) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and (9) the categories of sources of records in the system. (**Chapter 508**)

**System Owner (SO)**
Individual responsible for daily program and operational management of their specific USAID system. SOs are responsible for ensuring that a security plan is prepared, implementing the plan, and monitoring its effectiveness. (**Chapter 508, 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 Web Sites and Applications**
Web-based technologies that are not exclusively operated or controlled by a government entity. Often these technologies are located on a ".com" Web site 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 Web site. (**Chapter 508**)

**Unauthorized Disclosure**
When PII is disclosed to anyone except the subject individual absent the written consent of the subject individual, unless the disclosure falls within one of twelve statutory conditions in the Privacy Act, 5 USC 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: United States Direct-Hire employees, Personal Services Contractors, Fellows, Participating Agency Service Agreement, 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.) (**Chapter 508, 547**)

508_083120