ADS Chapter 508

Privacy Program

Partial Revision Date: 09/15/2014
Responsible Office: M/CIO/IA
File Name: 508_091514

Functional Series 500 – Management Services
ADS 508 – Privacy Program
POC for ADS 508: Meredith Snee, (703) 666-1247, msnee@usaid.gov

Table of Contents

508.1 OVERVIEW

Effective Date: 03/07/2014

This ADS chapter provides the organization, functions, policies, and procedures of the USAID Privacy Program.

Safeguarding personally identifiable information (PII) in the possession of USAID and preventing its misuse are essential to ensure that USAID retains the trust of the American public. The USAID responsibility to the American public is a function of the **Privacy Act of 1974** and the federal privacy authorities that flow from it, including the **E-Government Act of 2002, Section 208**.

The Privacy Program supports USAID missions and business functions 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.

USAID must protect PII against anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness either to an individual or to USAID. To accomplish that requirement, USAID must incorporate privacy analyses into each stage of the information life cycle.

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

508.2 PRIMARY RESPONSIBILITIES

Effective Date: 03/07/2014

USAID will only be successful in protecting PII as long as all USAID offices and employees are committed to working daily to incorporate privacy considerations into their program functions and activities. The following descriptions are the general responsibilities of USAID officials and employees. Specific role-based responsibilities appear throughout ADS 508. For additional information and answers to basic questions about the responsibilities to protect the privacy of information about individuals, see **ADS 508saa, Privacy Basics**.

a. The **Senior Agency Official for Privacy (SAOP) (AA/M)** 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.

b. The **Chief Privacy Officer (CPO) (M/CIO/IA)** provides oversight over and guidance for privacy policy and procedures, compliance activities, reporting, and the effectiveness of the Agency-wide Privacy Program, as well as ensuring that the analysis of privacy issues are incorporated into each stage of the information life cycle.

c. The **Privacy Act Implementation Officer (PAIO) (M/CIO/IA)** serves as the principal point of contact for Privacy Office policy and operations, supervises Privacy Office analysts, and manages the implementation of USAID privacy protection plans and procedures.

d. The **Privacy Office (M/CIO/IA)** is responsible for day-to-day privacy activities, including compliance documentation, such as Privacy Threshold Analyses, Privacy Impact Assessments, 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.

e. The **Chief Information Security Officer (CISO) (M/CIO/IA)** is responsible for managing the monitoring of USAID systems for privacy breaches and the reporting of USAID privacy incidents through the USAID Computer Security Incident Response Team (CSIRT).

f. The **Computer Security Incident Response Team (CSIRT) (M/CIO/IA)** monitors USAID systems for data breaches and reports USAID privacy incidents to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery.

g. 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 nongovernment Web site, and branding and marking the USAID presence on third-party Web sites.

h. The **Office of the General Counsel (GC)** interprets privacy statutes, regulations, and other legal authorities and reviews reports, systems of records notices, 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.

i. The **Office of Acquisition and Assistance (M/OAA)** ensures that USAID contracting documents have the appropriate information privacy clauses sufficient to ensure contractor compliance with federal privacy authorities and protection of the PII collected, used, maintained, and disseminated by USAID.

j. The **Office of the Inspector General (OIG)** monitors the integrity, efficiency, and effectiveness of USAID Privacy Program policies, activities, and reporting.

k. The **Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD)** is responsible for submitting required USAID privacy documentation to the *Federal Register* and for managing and responding to Privacy Act access and amendment requests.

l. Program Managers (PMs) are responsible for ensuring the privacy and security of the PII that their programs collect, use, maintain, and disseminate and for complying with federal privacy authorities.

m. System Owners (SOs) are responsible for ensuring the privacy and security of the PII that their information systems collect, use, maintain, and disseminate and for complying with federal privacy authorities.

n. System of Records Managers are responsible for ensuring the privacy and security of the PII that their Privacy Act Systems of Records collect, use, maintain, and disseminate and for complying with federal privacy authorities.

o. Information System Security Officers (ISSOs) are responsible for ensuring the security of the PII that their programs collect, use, maintain, and disseminate and for complying with federal privacy authorities.

p. Mission Privacy Liaisons are responsible for ensuring the privacy and confidentiality of the PII that their mission programs and employees collect, use, maintain, and disseminate and for complying with federal privacy authorities.

q. USAID Agreement Officers ensure that USAID interagency agreement documents have the appropriate information privacy clauses sufficient to ensure agency service provider compliance with federal privacy authorities and protection of the PII collected, used, maintained, and disseminated by USAID.

r. USAID Supervisors are responsible for instructing, training, and supervising employees on safeguarding PII and may be subject to disciplinary action for failure to take appropriate action upon discovering a breach or failure to take required steps to prevent a breach from occurring.

s. USAID Employees are 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 breaches of PII, and to reduce the volume and types of PII to only that needed for program functions.

508.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

508.3.1 Personally Identifiable Information (PII)

Effective Date: 03/07/2014

Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., alone, or when combined with other personal or identifying

information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

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 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.

PII examples include name, address, SSN, or other identifying number or code, telephone number, and e-mail 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 defining PII for USAID purposes, 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: 03/07/2014

This section explains the framework for the policies and activities of the USAID Privacy Program.

508.3.2.1 Fair Information Practice Principles
Effective Date: 03/07/2014

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 are the Fair Information Practice Principles (FIPPs). 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 life cycle.

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. Only collect 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: 03/07/2014

Using the FIPPs, the National Institute for Standards and Technology (NIST) has developed guidance regarding privacy controls in ***Security and Privacy Controls for***

***Federal Information Systems and Organizations*, NIST SP 800-53, Rev. 4, *Appendix J: Privacy Controls* (April 2013)**. The Privacy Controls provide 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 Controls establish a relationship between privacy and security controls for the purposes of enforcing privacy and security requirements within the NIST Risk Management Framework.

ID	Privacy Controls
AP 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 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 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 Date Integrity Board
DM 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
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP 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

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

508.3.2.3 No Expectation of Privacy on USAID Information Systems

Effective Date: 03/07/2014

Users have no reasonable expectation of privacy when using USAID information systems. USAID alerts users of all USAID 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:

- You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. 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.

- Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except USAID Chief Information Officer (CIO).

508.3.3 Privacy Rules of Behavior

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: 03/07/2014

All USAID employees are responsible for protecting PII from unauthorized exposure and for reducing the volume and types of PII necessary for program functions. Employees must protect any PII that they handle, process, compile, maintain, store, transmit, or report on in their daily work. To protect PII, employees must use proper collection, storage, transportation, transmission, and disposal methods; must not access PII beyond what they need to complete their job duties; and 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. Employees must label documents containing PII with the SBU header and footer and use the green SBU Cover Sheet (AID 630-3) 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 have access.

Failure to protect PII may result in administrative sanctions, and criminal and/or civil penalties. Employees 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.

It is important to emphasize that a few simple and cost-effective steps may well deliver the greatest benefit against abuse, loss, or theft. For more information about an employee'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 employees must report immediately upon discovery *all potential and actual* privacy breaches to both the CIO Helpdesk at (202) 712-1234 or **CIO-HELPDESK@usaid.gov** ***and*** the Privacy Office 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 Office at **privacy@usaid.gov**.

508.3.3.2 Privileged and Manager IT Rules of Behavior

Effective Date: 03/07/2014

This section addresses USAID's policy requirements for the behavior of 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 life cycle (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. For this purpose, Managers must complete a Privacy Threshold Analysis (PTA) at the early program or system design phase and might need to prepare additional privacy compliance documentation. To be comprehensive and meaningful, PTAs and other privacy compliance documentation require collaboration by program experts as well as experts in the areas of information technology, IT security, records management, 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 and for PII, System Owners must incorporate privacy compliance requirements into the Security Assessment & Authorization (SA&A) process, which is an evaluation of an IT system's 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. With the incorporation of the Privacy Control Catalog into **NIST SP 800-53, Rev. 4** at Appendix J, and USAID adoption of Revision 4, System Owners are must ensure that privacy compliance issues are a part of the SA&A process starting with the PTA at the start of the SA&A process.

Information System Security Officers 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 instructing, training, and supervising employees on safeguarding PII and may be subject to disciplinary action for failure to take appropriate action upon discovering a breach or failure to take required steps to prevent a breach from occurring. For more information about an employee'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, following due process, in accordance with **ADS 485, Disciplinary Action - Foreign Service** and **ADS 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct - Civil Service**.

508.3.4 Authority and Purpose

Effective Date: 03/07/2014

USAID uses the PII Inventory, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), Privacy Act Section (e)(3) Statement (Privacy Act Statement) (also known as Privacy Act Notice), 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 Accountability, Audit, and Risk Management

Effective Date: 03/07/2014

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

508.3.5.1 Privacy Threshold Analyses

Effective Date: 03/07/2014

This section addresses USAID's policy requirements for the creation and maintenance of Privacy Threshold Analyses (PTAs).

All employees are responsible for protecting the PII entrusted to their care. The Privacy Office uses PTAs to determine how USAID programs handle PII to ensure that employees fulfill their PII protection responsibilities. Program Managers and System Owners must conduct PTAs using the 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. The PTA Template contains guidance on how to conduct a PTA. For more information about PTAs, see **ADS 508maj, USAID Privacy Threshold Analysis Template**.

The Privacy Office uses the PTA to (1) determine whether a particular program will encounter any privacy risks as it performs its functions; and (2) identify whether the program needs to comply with any privacy protection requirements pursuant to federal

privacy statutes, regulations, and other authorities. The Privacy Office uses the PTA 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.

508.3.5.2 Privacy Impact Assessments

Effective Date: 03/07/2014

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 must conduct a PIA when it uses information technology (systems) to collect, use, maintain, or disseminate PII.

Under OMB Memorandum M-03-22, USAID must conduct a PIA before developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or initiating (consistent with the Paperwork Reduction Act), a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

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 - 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 **ADS 508mac, USAID Privacy Impact Assessment Template**.

The Privacy Office uses the PIA to (1) determine the risks and effects of collecting, using, maintaining, 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. A System Owner must demonstrate through the PIA, for any new system that involves PII, that they conducted an in-depth analysis to ensure that they have built privacy protections into the system.

USAID must update PIAs to reflect changed information collection authorities, business processes or other factors affecting the PII. In addition, USAID 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 an 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. However, USAID programs may prepare one PIA to cover multiple third-party Web sites or applications that are functionally comparable, as long as USAID's practices are substantially similar across the third-party Web sites and applications.

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 life cycle 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.

508.3.5.3 Privacy Considerations for Contracts

Effective Date: 03/07/2014

Pursuant to the **Privacy Act** Section(m)(1), the Office of Acquisitions and Assistance (OAA) must work with Program Managers, System of Records Managers, and System Owners to include in contracts appropriate privacy protection language in order to ensure contractor compliance with the Privacy Act and the federal authorities that flow from it, including the **E-Government Act Section 208**. **The Federal Acquisition Regulation (FAR) (48 CFR) Part 24, Protection of Privacy and Freedom of Information** and **52.239–1 Privacy or Security Safeguards**, is the mechanism that requires OAA to insert certain language in contracts to ensure compliance with the **Privacy Act of 1974**.

In addition, OAA must work with Program Managers, System of Records Managers, and System Owners to consider the following privacy protections in contracts:

a. USAID ownership and control of PII in systems for the length of the contract and beyond;

b. Contractor or service provider has no ownership of the PII;

c. Contractor or service provider has no access or retention rights to the PII beyond those authorized by the contract and only during the life of the contract;

d. Contractor or service provider must provide USAID access to PII when needed; and

e. Describe the responsibilities and liabilities of the contractor or service provider and for USAID for PII incidents and breach response activities.

508.3.5.4 Privacy Considerations for Interagency Agreements

Effective Date: 03/07/2014

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 Program Managers, System of Records Managers, and System Owners to consider the following privacy protections in interagency agreements:

a. USAID ownership and 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.

508.3.5.5 Privacy Considerations for Cloud Computing Services

Effective Date: 03/07/2014

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. OAA must work with Program Managers, System of Records Managers, and System Owners to include in contracts appropriate privacy protection language to:

a. Limit the right of the cloud services provider to change the terms at will, which could alter the privacy risks during the life of the contract; 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 US, 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, so USAID should gather privacy requirements as early as possible in the information life cycle to understand fully how USAID will ensure that a cloud services provider maintains its duty to protect PII.

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 provides **Standard Contract Language** that 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**.

508.3.5.6 Incorporating Privacy into the Information Life Cycle

Effective Date: 03/07/2014

OMB has directed USAID to incorporate privacy analyses into each stage of the information life cycle (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 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 life cycle 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 life cycle 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's 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. With the incorporation of the Privacy Control Catalog into **NIST SP 800-53, Rev. 4** at Appendix J, and USAID adoption of Revision 4, privacy compliance issues will become part of the SA&A process starting with the Privacy Threshold Analysis (PTA) at the start of the SA&A process.

508.3.5.7 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.

USAID has implemented an automated data-loss-prevention (DLP) tool that is able to discover, monitor, and protect PII wherever it is stored or used across USAID systems. The DLP tool provides an enterprise-wide approach to the protection of electronic PII to mitigate risks from PII loss to individuals and USAID business operations and assets. The DLP tool to monitors how PII is used and where it goes in order to protect PII by automatically enforcing data loss policies; educating users about data security; securing exposed data; and stopping data leaks.

USAID currently uses the DLP tool to monitor continuously the USAID-managed email network to detect and prevent the movement of PII out of USAID-controlled networks. The Privacy Office creates the privacy policy and procedures for the DLP tool, while the USAID Computer Security Incident Response Team (CSIRT) uses the DLP tool to monitor the USAID email system for privacy breaches due to unauthorized disclosure of PII outside of USAID. The Privacy Office identifies and responds to privacy breaches using the data provided by the CSIRT.

508.3.5.8 Privacy Awareness Training

Effective Date: 03/07/2014

USAID must provide annual privacy awareness training to all USAID employees and contractors. All employees must complete annual privacy awareness training. This annual training provides employees and a better understanding of the basic knowledge necessary for protecting PII data elements in accordance with USAID and Privacy Act requirements. If employees do not complete their annual privacy awareness training,

the Chief Privacy Officer (CPO) will suspend their access to such Privacy Act information data elements.

In addition, USAID provides targeted, role-based training to those employees and contractors designated as PII custodians, who will use or view PII data elements in the routine performance of their jobs.

508.3.5.9 Privacy Reporting
Effective Date: 03/07/2014

The USAID Senior Agency Official for Privacy (SAOP) reports to OMB on a quarterly and annual basis according to the requirements of the Federal Information System Management Act (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 **ADS 508.3.1, Personally Identifiable Information (PII).** For more information on the threshold for conducing PIAs, see **ADS 508.3.5.3, Privacy Impact Assessments**. For more information on the threshold for creating SORNS, see **ADS 508.3.10.2, System of Records Notices**.

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

508.3.6 Data Quality and Integrity
Effective Date: 03/07/2014

USAID must take reasonable steps to protect the quality 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.

508.3.6.1 Data Quality
Effective Date: 03/07/2014

USAID System of Records Managers must exercise due care in ensuring that records containing PII are accurate, complete, timely, and relevant for Agency purposes. This is necessary to assure fairness in any determination about an individual.

508.3.6.2 Data Integrity
Effective Date: 03/07/2014

USAID System of Records Managers must implement security and privacy controls to maintain the accuracy and consistency of PII throughout the information life cycle. This is necessary to assure fairness in any determination about an individual.

508.3.6.3 Matching Programs and Agreements
Effective Date: 03/07/2014

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)**.

508.3.6.4 Data Integrity Board
Effective Date: 03/07/2014

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 Data Minimization and Retention
Effective Date: 03/07/2014

USAID must collect, use, and retain only 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.

All Employees must use PII properly, and for reducing their use of PII and the volume and types of PII they collect. Employees must also retain PII only as long as necessary to accomplish their program purposes.

508.3.7.1 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 Number (SSNs), the Privacy Office 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 Office 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 Office 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-07-16**.

508.3.7.2 Storage and Destruction of PII

Effective Date: 03/07/2014

All employees must carefully store and destroy PII and media containing PII by approved methods. Employees 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. Specifically, employees must destroy PII documents by shredding, and must store and destroy media containing PII in accordance with methods described in **ADS 545mak, Data Remanence Procedures**, and **ADS 545mas, Media Handling Procedures and Guidelines**.

508.3.8 Individual Participation and Redress

Effective Date: 03/07/2014

This section addresses the policy requirements for Individual Participation and Redress. 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.

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 guarantees an individual three primary rights: (1) To see 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 sue the federal government for violations of the Privacy Act, such as permitting unauthorized persons to read an individual's records.

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 (U.S.

citizens and lawfully admitted permanent resident aliens). The FOIA, on the other hand, covers virtually all records in the possession and control of federal executive branch agencies. 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 Security

Effective Date: 03/07/2014

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

508.3.9.1 Inventory of Personally Identifiable Information

Effective Date: 03/07/2014

USAID must review its PII holdings periodically 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 Privacy Office has created and updates periodically 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 Office 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.

508.3.9.2 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 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.

508.3.9.3 Encrypting PII

Effective Date: 03/07/2014

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 (Blackberries and iPhones). For more information about encrypting PII, see the **ADS 545, Information Systems Security,** section **545.3.3.17(e)**, Protecting Privacy Sensitive Systems.

Employees must ensure that PII is encrypted on all removable media, such as CDs and DVDs. Employees must also remove all PII from email strings and encrypt, using Adobe Acrobat or WinZip, all PII in email attachments sent from USAID approved domains, which include only usaid.gov, state.gov, ofda.gov, and oti.gov. For more information about encrypting PII, see the **ADS 545, Information Systems Security,** section on Protecting Privacy Sensitive Systems and see **ADS 545mbd, Rules of Behavior for Users**.

508.3.9.4 Privacy Breach Reporting and Response

Effective Date: 03/07/2014

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. Therefore, incidents involving a breach of PII have a critical time-period for reporting.

All employees must report immediately upon discovery *all potential and actual* privacy breaches to both the CIO Helpdesk at 202-712-1234 or **CIO-HELPDESK@usaid.gov** ***and*** the Privacy Office 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. The USAID Privacy Office evaluates the incident. If the Privacy Office determines that USAID must report the incident, the Privacy Office submits a report to the USAID

Computer Security Incident Response Team (CSIRT), which reports the incident to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery or detection.

A privacy breach occurs if there is unauthorized access to or collection, use, disclosure or disposal of personal information. The most common privacy breaches occur when personal information of customers, clients, or employees is lost, stolen or mistakenly disclosed. Breaches subject to notification requirements include a breach of PII in any formant (e.g., paper, electronic, mobile media, etc.). In addition, an effective response necessitates notification of the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notifying the affected individuals or playing a role in preventing or minimizing harms from the breach. For example, a PII breach could involve a lost or stolen laptop or mobile device containing PII, or mistakenly sending an unencrypted e-mail containing PII to the wrong person.

For more information about privacy breach reporting and response, see **ADS 508mai, USAID Privacy Program Breach Notification Policy and Plan** and **ADS 545, Information Systems Security**.

508.3.10 Transparency
Effective Date: 03/07/2014

USAID must provide public notice of its information practices and the privacy impact of their 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, PTAs, PIAs, and SORN on USAID public Web sites.

508.3.10.1 Privacy Act Section (e)(3) Statements or Notices
Effective Date: 09/15/2014

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

508.3.10.2 Systems of Records Notices

Effective Date: 03/07/2014

This section addresses the policy requirements for Systems of Records Notices under the **Privacy Act**. USAID must conform to the notice requirements of the **Privacy Act of 1974**.

The Privacy Act applies to "systems of records", which are USAID-maintained IT systems or paper files that contain information on individuals ("Privacy Act records"), where the information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular 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 Office 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**.

508.3.10.3 Privacy Issues with Information Collection Requests

Effective Date: 03/07/2014

This section addresses the policy requirements for the privacy issues related to the 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 representative of the types of ICRs subject to the 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 Chapter 508 sections for more information: PTAs, PIAs, SORNs, and Privacy Act Statements.

508.3.10.4 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.

System Owners 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. System Owners 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.

Systems Owners 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 System Owners correct the deficiencies. For more information about System Owner responsibilities regarding USAID public Web site privacy policies, see **ADS 508mak, USAID Public Web Site Privacy Policies Requirements**.

508.3.10.5 Third-Party Web sites and Applications

Effective Date: 03/07/2014

USAID must take specific steps to protect individual privacy whenever it uses 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 nongovernment 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 imbedded in the USAID web site.

d. **Agency Branding.** System Owner must apply appropriate branding to distinguish USAID activities from those of nongovernment 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.

508.3.11 Use Limitation
Effective Date: 03/07/2014

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 suffer 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**.

508.3.11.1 Open Government and Open Data
Effective Date: 03/07/2014

USAID must manage its information as an asset throughout the information life cycle to promote openness and interoperability, and, wherever possible and legally permissible, to ensure that data released to the public is easy to find, accessible, and usable. In order to implement these open data requirements, USAID must incorporate a full analysis of privacy risks into each stage of the information life cycle to identify information that should not be released.

The Privacy Office uses the **USAID Open Data Privacy Analysis Template** to determine how USAID programs handle PII under OMB open government and open data guidance to ensure that employees fulfill their PII protection responsibilities. The USAID program office that owns the dataset must complete the **USAID Open Data Privacy Analysis Template** before posting datasets on Web sites available to the public, and thereafter periodically, before updating datasets on Web sites available to the public.

The Privacy Office uses the completed **USAID Open Data Privacy Analysis Template** to (1) determine whether a particular dataset involves privacy risks; and (2) identify what privacy protection actions the program must take before it posts the dataset on a Web site available to the public. The program responsible for the dataset must determine whether a particular dataset contains PII and must comply with all privacy protection requirements, such as removing PII from the dataset and the metadata associated with that dataset, before posting the dataset to a web site available to the public.

The **USAID Open Data Privacy Analysis Template** contains guidance on how to complete the Template. For more information, see **ADS 508mah, USAID Open Data Privacy Analysis Template**.

508.3.11.2 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**.

508.3.11.3 Privacy Act Disclosure Limitations and Routine Uses
Effective Date: 03/07/2014

The Privacy Act prohibits the disclosure of any PII 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)**. 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.

508.3.11.4 Privacy Act Disclosure Exemptions
Effective Date: 03/07/2014

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 principle 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**.

508.3.11.5 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 Privacy Act of 1974 at **22 CFR 215.12**.

508.4 MANDATORY REFERENCES

508.4.1 External Mandatory References

508.4.1.1 Statutes and Regulations

Effective Date: 03/07/2014

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

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

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

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

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

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

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

l. Health Information Portability and Accountability Act of 1996, (Public Law 104-191)

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

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

508.4.1.2 Office of Management and Budget (OMB)

Effective Date: 03/07/2014

a. OMB Circular A-130 Appendix I, Section 4a, 4b – Agency Biennial Privacy Act Report and Agency Biennial Computer Matching Report; and Appendix III, Security of Federal Automated Information Resources

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

c. OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites

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

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

f. OMB Memorandum M-05-04, Policies for Federal Agency Public Web sites

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

h. OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information

i. OMB Memorandum M-06-16, Protection of Sensitive Agency Information

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

k. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

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 Web sites 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

508.4.1.3 National Institute of Science and Technology (NIST)

Effective Date: 03/07/2014

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

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

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

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

e. 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: 09/15/2014

a. ADS 103, Delegations of Authority

b. ADS 306, Interagency Agreements

c. ADS 485, Disciplinary Action - Foreign Service

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

e. ADS 505, Forms Management Program

f. ADS 506, Reports Management

g. ADS 507, Freedom of Information Act

h. ADS 508maa, USAID System of Records Notice Template

i. ADS 508mac, USAID Privacy Impact Assessment Template

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

k. ADS 508mah, USAID Open Data Privacy Analysis Template

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

m. ADS 508maj, USAID Privacy Threshold Analysis Template

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

o. ADS 516, Federal Register Notices

p. ADS 545, Information System Security

q. ADS 545mak, Data Remanence Procedures

r. ADS 545mas, Media Handling Procedures and Guidelines

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

t. **ADS 557, Public Information**

u. **ADS 557mac, Updated Privacy Policy for USAID Information Technology Systems**

508.5 Additional Help

Effective Date: 03/07/2014

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

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

c. **FedRAMP Standard Contract Language**

508.6 DEFINITIONS

Effective Date: 03/07/2014

The terms and definitions listed below have been incorporated into the ADS Glossary. See the **ADS Glossary** for all ADS terms and definitions.

access
The ability or opportunity to gain knowledge of personally identifiable information. (**Chapter 508**)

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 representing the U.S. Government through the exercise of his/her delegated authority to enter into, administer, and/or terminate contracts and make related determinations and findings. This authority is delegated by one of two methods: to the individual by means of a "Certificate of Appointment," SF-1402, as prescribed in FAR 1.603-3, including any limitations on the scope of authority to be exercised, or to the head of each contracting activity (as defined in AIDAR 702.170), as specified in AIDAR 701.601. (**Chapters 302**, **306**, **331**, **508**)

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 and 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**)

contractor
This term refers to independent contractors and institutional contractors. (**Chapter 508**)

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**)

employees
Includes USAID direct-hire personnel, fellows, detailees, interns, Personal Service Contractors (PSC), Participating Agency Staff (PASA), and any other category of person, not a contractor, requiring a security clearance to work on USAID information or material or have unescorted access in USAID space. (**Chapter 508**)

encryption
This is the act of transforming information into an unintelligible form, specifically to obscure its meaning or content. (**Chapters 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 ten 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 life cycle
The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition. (**Chapters 508** and **545**)

information system (IS)
The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. This term includes both automated and manual information systems. (**Chapters 502**, **508**, **545**, **552**, **562**, **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. **(Chapters 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 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 a 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). (**Chapters 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)
Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Same as "information in an identifiable form" and records about individuals in a "system of records".

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**)

PII custodian
Any USAID staff member who handles PII in the routine execution of daily work responsibilities. (**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. (**Chapters 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 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 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. (**Chapters 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 Analysis (PTA)
Analysis of whether a program or system has privacy implications, and if additional privacy compliance documentation is required, such as a Privacy Impact Assessment or System of Records Notice. (**Chapters 508** and **545**)

Program Manager (PM)
Government official responsible and accountable for the conduct of a government program. A government program may be large (e.g., may provide U.S. assistance to other nations); it may also be a support activity such as the Agency's personnel or payroll program. **(Chapters 508, 545, 552, 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)
Sensitive but unclassified (SBU) information is information that is not classified for national security reasons, but that warrants/requires administrative control and protection from public or other unauthorized disclosure for other reasons. SBU should meet one or more of the criteria for exemption from public disclosure under the **Freedom of Information Act** (FOIA) (which also exempts information protected under other statutes), 5 U.S.C. 552, or should be protected by the **Privacy Act**, 5 U.S.C. 552a. (**12 FAM 540, Sensitive But Unclassified Information**) **(Chapters 508** and **545**)

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: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. (**Chapter 545**) 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 102, 413, 508**)

system
Refers to any information system or application, and may be used to designate both the hardware and software that comprise it. (**Chapters 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 shall include— (A) the name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; (H) 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 (I) 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. System Owners are responsible for ensuring that a security plan is prepared, implementing the plan and monitoring its effectiveness. (**Chapters 508** and **545**)

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**)

508_091514