ADS Chapter 508

The USAID Privacy Policy

Hyperlink Check Date: 03/21/2012
Partial Revision Date: 08/08/2011
Responsible Office: M/CIO/CISO-CPO
File Name: 508_032112

Functional Series 500 – Management Services
ADS 508 – The USAID Privacy Policy Program

Table of Contents

*An asterisk and yellow highlight indicate that the adjacent information is new for this chapter or substantively revised.

*508.1 USAID PRIVACY POLICY OVERVIEW

Effective Date: 12/08/2009

This ADS chapter details the policy directives and required procedures of the USAID Privacy Policy Program. USAID's privacy stance in regard to the protection of personally identifiable information (PII) and privacy-related protections of its employees and business partners complies with the **Privacy Act of 1974 (Privacy Act)**, as amended.

The Privacy Act mandates that all Federal agencies protect PII collected, maintained, or disseminated by an agency from unauthorized disclosure in both electronic and paper records. The Act also specifies to whom such information can be disclosed. . Specifically, the Privacy Act states that Federal agencies must establish a set of "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of (the Privacy Act), including any other rules and procedures adopted pursuant to (the Privacy Act) and the penalties for noncompliance." (See **5 U.S.C. section 552a(e)(9)** and **OMB M-07-16.**)

The Privacy Act allows individuals to gain access to most of their personal information maintained by Federal organizations and to seek amendment of their records for any inaccurate, incomplete, untimely, or irrelevant information. (See **5 U.S.C. section 552a(e)(5).**)

*This ADS chapter adheres to the Office of Management and Budget (OMB) Memorandum (M) 10-06 that promotes the Transparency and Open Government Directive. The intent of **OMB M-10-06** is to direct executive departments and agencies to take specific actions to implement the principles of transparency, participation, and collaboration. However, satisfying Open Government objectives does not suggest that the presumption of openness precludes the legitimate protection of information whose release would threaten national security, invade personal privacy, breach confidentiality, or damage other genuinely compelling USAID interests. (See **OMB M-10-06**.)

Additionally, USAID must follow the guidelines set forth in the **Freedom of Information Act** (FOIA) and outlined in a **March 19, 2009 Memo from the Attorney General**. (For more details related to the USAID Open Government plan and initiative, see the **USAID Open Government Web site).** For more details related to **USAID Privacy Basics**, see the Additional Help Reference for ADS 508. USAID must also comply with **508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d)** for access to information systems.

508.2 PRIMARY RESPONSIBILITIES

Effective Date: 08/31/2007

The Privacy Act and subsequent statutory and regulatory guidance established privacy-specific roles and responsibilities for Government department and agencies. USAID privacy-specific personnel roles and responsibilities are described below.

a. The **Administrator of USAID (A/AID)** is responsible for establishing a federally compliant Privacy Policy Program that complies with Federal law and OMB guidance and directives.

b. The **Chief Privacy Officer (CPO)** serves as the principal point of contact for privacy policy issues related to information technology and Web matters.

c. The **Privacy Act Implementation Officer (PAIO)** serves as the principal point of contact for day-to-day Privacy Policy Program operations and is responsible for the implementation of USAID privacy protection plans and procedures.

d. The **Bureau for Legislative and Public Affairs (LPA)** provides assistance, as required by the CPO, in the review of privacy policies and procedures with respect to public Web sites.

e. The **Office of the General Counsel (GC)** provides assistance, as required by the CPO, in reviewing reports, systems of records notices, proposed rules, and other related matters that USAID submits to Congress, OMB, or other parties.

f. The **Office of the Inspector General (OIG)** provides oversight duties for the Privacy Policy Program, which includes periodic review of the privacy policy and reporting as required by Congress, OMB, and other parties.

g. **System Owners (SO)** have numerous responsibilities for systems that contain PII. These responsibilities are described throughout this chapter.

.

h. The **Bureau for Management, Management Services, Information and Records Division (M/MS/IRD)** is responsible for submitting required USAID privacy documentation to the Federal Register.

i. **USAID Employees** are responsible for protecting PII data that is entrusted to their care from unauthorized exposure. In accordance with OMB M-07-16, the USAID Privacy Policy Program has a responsibility to "*reduce the volume of personally identifiable information*" used by USAID System Owners and applications.

508.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 08/31/2007

This section details the policy directives and required procedures of USAID's Privacy Policy Program.

508.3.1 Roles and Responsibilities of the USAID Privacy Policy Program

Effective Date: 08/31/2007

a. The **Administrator of USAID (A/AID)** is responsible for:

(1) Delegating a designated Chief Privacy Officer who has centralized USAID-wide privacy policy program oversight and authority;

(2) Developing and implementing a fully integrated Privacy Policy Program and effective privacy management structure that demonstrates USAID's priority for protecting USAID employees and business partners' privacy;

(3) Ensuring that annual general privacy policy awareness training is provided to all USAID staff members who have routine access to or come in contact with PII data while performing their jobs; and provide role-based training to individuals who have been assigned additional responsibilities that require the handling of PII data;

(4) Identifying the senior USAID official(s) primarily responsible for coordinating and implementing USAID information technology, Web, and privacy policies;

(5) Being made aware of the identity of individuals who have day-to-day responsibilities for implementing USAID privacy policy;

(6) Designating reviewing officials for USAID Privacy Impact Assessments (PIA); and

(7) Establishing an USAID Breach Response Team.

b. The **Chief Privacy Officer (CPO)** is responsible for:

1. Maintaining oversight of the USAID Privacy Program to ensure that it is in compliance with all applicable statutory and regulatory guidance (listed in section **508.4** of this chapter);

2. Establishing new, and enforcing current, privacy policy requirements to include developing and disseminating privacy policy updates, plans, and procedures;

3. Implementing and sustaining USAID-wide technical safeguard mechanisms for systems that use, share, collect, transfer, store, or disclose privacy information;

4. Maintaining appropriate data quality in privacy information documentation such as SORNs, PIAs, annual evaluations, incident handling reports;

5. Conducting periodic audits and reviews to identify deficiencies, weaknesses, or risks;

6. Establishing an education and training program on privacy and data protection policies, and evaluating those policies annually for compliance with statutory and regulatory guidance;

7. Evaluating annually the effectiveness of the procedures for conducting PIAs, and actively using those evaluation results to improve USAID PIA procedures;

8. Evaluating legislative and regulatory proposals that define the use, collection, and disclosure of PII by Federal agencies;

9. Preparing internal and external reports detailing USAID activities related to protection of PII, and to include complaints filed related to privacy violations, implementation of section 552a of Title 5 of United States Code (USC) internal controls;

10. Providing arbitration and escalation assistance of privacy requests with the assistance of the General Counsel (GC);

11. Promptly, efficiently, and effectively implementing privacy policies that reduce PII data collection burdens on the general public;

12. Reviewing publications and forms, including:

1. Reviewing and approving Information Collection Requests (ICR) containing PII;

2. Approving and Publishing Privacy Impact Assessments,

3. Creating and publishing System of Records Notices (SORNs);

13. Responding to all inquiries made during the consultative/review process with SOs.

c. The **Privacy Act Implementation Officer (PAIO)** is responsible for:

1. Assisting SOs in conducting PIAs;

2. Processing Privacy Act inquiries and requests;

3. Reporting annually to the CPO on USAID compliance with section 208 of the **E-Government Act of 2002**, to include the following:

- Listing all systems and information collections for which a PIA was made publicly available as posted on the USAID Privacy page, Federal Register, or other Federal managed Web site),

- Maintaining a current list of principal USAID privacy points of contact, including names and titles, for annual reporting; and

4. Maintaining overall custodianship of protected records and data.

d. The USAID **Bureau of Legislative and Public Affairs (LPA)** is responsible for:

1. Reporting annually to the CPO on USAID compliance with section 208 of the **E-Government Act of 2002**, to include the following:

- Listing all systems or information collections for which a PIA was made publicly available (such as, posted on the USAID Privacy page, Federal Register, or other Web site);

- Describe all usage of persistent Web browser/Internet "*cookies*" at USAID;

2. Reporting on the progress of implementing machine readability technology(s) associated with publicly facing Web sites; and

3. Verifying that USAID privacy policy pages on publicly accessible Web sites contain code that enables accessibility devices to automatically read the policy.

e. The **Office of the Inspector General (OIG)** is responsible for carrying out USAID statutory responsibilities pursuant to the **Privacy Act**, **U.S.C. section 522 of the Consolidated Appropriations Act of 2005**, and other statutory and regulatory guidance for privacy protections.

f. System Owners (SOs) and managers for major and minor USAID applications, general support systems, Web sites, databases, or other USAID information systems containing PII data elements are responsible for:

1. Verifying that systems under their responsibility operate in compliance with Federal privacy laws and this privacy policy, to include conducting privacy impact assessments (PIAs) for USAID systems and Web sites; and filing a System of Records Notice (SORN), if applicable.

2. Revalidating PIAs annually, or when a significant change is made to the information system or PII data elements collected, shared, maintained, or transmitted by the information system of record.

3. Establishing administrative, technical, and physical controls necessary for the secure physical storage of records to prevent acts of unauthorized access or disclosure, and physical damage or destruction; and

4. Conducting a Certification and Accreditation (C&A) of all systems that are storing, processing, or transmitting PII data to validate that appropriate security controls, as designated by the applicable **Federal Information Processing Standard (FIPS) 199** risk assessment categorization of the system of records is applied and the systems are operating as designed.

Information about the USAID certification and accreditation (C&A) processes are provided in **ADS 545, Information Systems Security**.

508.3.2 Privacy Act Awareness Training

Effective Date: 08/31/2007

The USAID CPO provides annual privacy awareness training to all USAID employees, particularly those employees who will use or view PII data elements in the routine performance of their jobs. In addition, USAID provides targeted, role-based training to those employees who have been designated as PII custodians.

In accordance with **OMB M-07-16**, a "Rules and Consequences Policy" must be developed to ensure that disciplinary actions levied against all managers, supervisors, and employees are fair. The Rules and Consequences Policy must inform and train all managers, supervisors and employees regarding their respective responsibilities relative to the safeguarding of personally identifiable information and the consequences and accountability for violating those responsibilities.

All USAID employees must complete annual privacy awareness training. This annual training is provided to employees so that they may better understand 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 CPO will suspend their access to such Privacy Act information data elements. If employees do not abide by the rules of behavior, their privileges to access such PII data will be denied.

*508.3.3 Privacy Impact Assessments

Effective Date: 06/25/2010

*This section addresses USAID's policy requirements for the creation and maintenance of Privacy Impact Assessment (PIA) statement documents as required by **OMB M-99-18**, **OMB M-03-22**, **OMB M-10-23** or a later OMB directive.

PIA statements are representative documents of the processes used to determine if USAID's information handling practices conform to established legal, regulatory, and policy frameworks for privacy protection. Information handling practices include both manual processes, as well as automated technology processes implemented by USAID.

When conducting a PIA, a CPO representative may assist System Owners on how to identify the following:

1. PII data elements contained within the system;

2. Risks to PII that may arise from the electronic collection and maintenance of such data;

3. Sharing of PII data elements with other departments or agencies, and

4. The physical security of the environment where PII is processed.

For systems or processes that contain or display PII information, System Owners must determine the appropriate protections, as defined by the system of records (**FIPS 199**), greater security categorization, or alternative methods utilized by USAID, to mitigate the identified risks.

USAID Privacy Office staff members can assist System Owners in conducting PIAs when such requests are coordinated through the USAID CPO or Deputy CPO offices. System Owners are responsible for conducting and/or updating the system of record's PIA for the following circumstances:

1. For every electronic information system and manual information collection system. The Privacy Office staff will assist System Owners in this identification process;

2. Before developing, procuring, or initiating IT systems that provide for the electronic collection of information from ten or more persons (excluding agencies or employees of the Federal Government);

3. When system changes, as defined by **NIST Special Publication (SP) 800-53a** or a later NIST directive, create a new privacy risk;

4. When other factors affecting the collection and handling of PII, information collection authorities, or business processes change; or

5. Once every three years for existing systems (meaning those that have operated without any significant changes).

The USAID Privacy Office staff will review and approve for signature each USAID PIA statement:

1. When the Privacy Office staff reviews and approves a PIA, they must notify the System Owner that the system has met USAID PIA requirements, and the PIA must be published to USAID's external Web site: **http://www.usaid.gov/index.html.**

2. If the Privacy Office staff reviews but does not approve a PIA, the Privacy Office must notify the System Owner that their system has not satisfied USAID's PIA requirements. A PIA must be completed successfully before the System Owner is permitted to allow the system to become operational.

System Owners must conduct their PIA using the USAID Privacy Office PIA template. That USAID PIA template can be downloaded from the USAID:

- Intranet,at **http://spsinternal.usaid.gov/m/cio/CISO/Pages/PrivacyForms.aspx [Note: This template is an internal USAID intranet document.]**,
- Privacy Office via e-mail request to **privacy@usaid.gov,** or
- Reviewed in Mandatory Reference 508mac,**Privacy Impact Assessment (PIA) Process and Procedures**.

*508.3.3.1 Third Party Privacy Impact Assessments

Effective Date: 06/25/2010

*This section, in accordance with **OMB M-10-23**, addresses the use of third-party Web sites or applications that provide or make PII data elements available to USAID. In general, USAID's use of any third-party Web site or application should be covered in a single, separate PIA. However, USAID may prepare one PIA document to cover multiple third-party Web sites or applications that are functionally comparable, as long as USAID's practices are substantially similar across each third party Web site or application.

[Please Note: USAID must take all practical steps to ensure that the USAID Privacy Notice is conspicuous, salient, clearly labeled, written in plain language, and prominently displayed at all locations where the general public might make PII available to USAID].

508.3.4 Information Collection Requests

Effective Date: 08/31/2007

The Paperwork Reduction Act (PRA) and subsequent regulatory guidance established requirements for information collection requests (ICRs). The PRA minimizes 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;

Subsequent PRA regulatory guidance includes:

- **The Privacy Act of 1974 (5 USC 552a);**

- **E-Government Act of 2002 (44 USC Chapter 36);**
- **The Children's Online Privacy Protection Act of 1998 (15 USC 6501-06);**
- **The Government Paperwork Elimination Act (P.L. 105-277, Title XVII);**
- **The Federal Information Quality Act (P.L. 106-554, Section 515);**
- **The Small Business Paperwork Reduction Act (44 USC 3520, P.L. 107-19);** and
- **OMB Memorandum M-00-15, Guidance on Implementing Electronic Signature in the Global and National Commerce Act, September 25, 2000;**

Surveys, questionnaires, registration forms, Web sites, and databases are representative of information collection requests systems. If such collection request systems are used by USAID, System Owners and/or applications are subject to the above PRA requirements.

ICRs are subject to the Privacy Act. See Section **508.3.5** of this chapter for additional details on System of Records requirements.

*508.3.4.1 Paperwork Reduction Act (PRA) Submission Worksheets

Effective Date: 08/31/2007

This section provides guidance for System Owners, who, with assistance from M/MS/IRD, must prepare and submit PRA Submission Worksheets to OMB for ICRs.

The **PRA section 3506 (2)(A)** requires that agencies publish a 60-day notice in the *Federal Register* to obtain public comment on the proposed collection, prior to submitting the information collection request to OMB. At the time of publication of the notice, USAID must have a draft survey instrument, at a minimum, available for the public for review. USAID System Owners must state in their ICRs whether any comments were received from the public, and that such comments will be addressed in the ICR submitted to OMB. Also, see ADS 508mab.

If the answer to any of the following questions is yes, then the System Owner must work with the USAID CPO staff to process an ICR As defined by PRA section3507(b):

1. "Are you collecting information from ten or more people (other than Federal employees)?

2. Is the information collected mandatory or required to obtain a benefit?

3. Is the information collected disclosed to the public or shared with a third party?

4. Does the information collection request PII data elements?"

M/MS/IRD must assist System Owners in developing ICRs to promote the reduction of information collected by USAID systems to only those data elements that are necessary for the function of the data collection system, application, or business process.

When submitting an ICR to OMB, USAID System Owners are required, by **PRA section 3507(b)**, to place a second notice in the *Federal Register* allowing for a 30 business day public comment period that informs the public that OMB approval is being sought and all comments should be submitted to OMB. This *Federal Register* notice runs concurrent with the first 30 business days of initial 60 business day OMB decision review. Therefore, USAID System Owners should allow at least 120 business days within the applicable project plan to allow for consideration of initial public comments, the second public comment period, and OMB review. Additional time must be allotted for preparation of an ICR, as well as publication delays normally associated with Federal *Register* notices.

Once approved, OMB issues a control number for the approved ICR. This control number must be displayed in the applicable USAID ICR on either the electronic or paper form used to collect the information or on the Web site page where the information was collected.

*See **Mandatory Reference 508mab,USAID Information Collection Request Process and Procedures** and **Mandatory Reference 508mad, Common Sense and Ad Hoc Requests**.

508.3.5 System of Records

Effective Date: 08/31/2007

The Privacy Act defines a system of records (SOR) as "*a group of records under the control of any agency from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual.*" A correctly designed SOR will have the following two key functional distinctions:

1. An indexing or retrieval capability that is built into the system; and

2. The Agency retrieves records about individuals by reference to a personal identifier, such as an individual's name or Social Security number (SSN) (See **OMB 7-16**).

For each USAID SOR, the System Owner must:

1. Permit individuals to seek legal remedies to enforce their rights granted under **The Privacy Act**;

2. Publish Federal Register notices describing all systems of records;

3. Make reasonable efforts to maintain accurate, relevant, timely, and complete records about individuals;

4. Not permit information collected about an individual for one purpose to be used for another purpose without giving notice to or getting the consent of the subject of the record, unless the record is being used as a routine use.

For each system of records maintained by a System Owner, he or she must

1. Maintain only PII considered relevant and necessary for the legally valid purpose for which it is obtained;

2. Where possible, collect information directly from the individual;

3. When a SOR is established or revised, prepare documentation for the Publications Officer to publish a notice in the Federal Register;

4. Update SORNs every three years or when a significant change occurs to the system that affects the privacy information maintained in that system;

5. Maintain records that are accurate, relevant, timely, and complete to ensure fairness to the individual of record;

6. Notify an individual when any USAID maintained record on that individual is made available to any person under a compulsory legal process that is a matter of public record;

7. Employ appropriate logical and physical security controls for the system to ensure confidentiality, integrity, and availability of records; and

8. Require personnel involved in the design, development, operation, or maintenance of any system of records, or maintaining such SORs, to sign a Rules of Behavior for each SOR for which they have been granted access. Additional Rules of Behavior information are provided in **ADS 545**.

SOR reporting requirements include providing details about:

- Uses of the collected information,
- Types of records maintained, and
- Inquiries and requests for access to the records.

USAID System Owners must file a System of Records Notice (SORN) and complete the entire Federal Register review period before the system will be permitted to operate in a production environment. System Owners must send all new SOR documentation or

significant alteration to an existing SOR to the USAID Privacy Office. The USAID Privacy Office staff will post the new SOR notice in the Federal Register for the System Owner. The Federal Register publication of SORNs allows interested persons to submit written data, views, or arguments to USAID.

Modification of information usage in a system with a SORN requires updating the existing SORN. The System Owner must provide the following information to the Privacy Office:

- A narrative report of the SOR, which includes notice of any new use or intended use of the information in the system, and a description of each routine use of the records contained in the system, including the categories of users and the purpose of such use;

- A Privacy Act Statement; and

- A System of Records Notice.

A minimum of 10 business days is required for proper CPO staff review. This USAID Privacy Office review is considered part of the 40-day notice period required by OMB. The USAID Privacy Office must post a notice with the Federal Register at least 40 days prior to the publication of the SORN.

For additional USAID processes, approved procedures, and templates, see **Mandatory Reference 508maa, Filing a System of Records Notice Process and Procedures**.

All privacy documentation must be in electronic format. System Owners must submit all privacy documentation via e-mail to **privacy@usaid.gov**. Alternatively, System Owners may mail properly protected electronic media containing privacy documentation to the following USAID address:

Attn: Chief Privacy Officer
United States Agency for International Development
Potomac Yards Two
2733 South Crystal Drive
11th Floor, Room 11114
Arlington, VA 22202

System Owners may submit questions or comments related to PIAs, USAID templates, SORNs, information collection procedures, or other PII data related topics to the Privacy Office through **privacy@usaid.gov**.

508.3.6 Web Privacy Policies

Effective Date: 08/31/2007

USAID Web privacy policies must comply with all OMB privacy-related memoranda and must include notice about the nature, purpose, use, and sharing of privacy related information on all official USAID Web sites.

System Owners are responsible for compliance with these privacy protection notifications and requirements for their Web sites. The following list provides Federal/USAID Web site privacy policy requirements:

1. Prominently Display a Privacy Act Statement

a. Notifies users of the purpose, authority for, and use of the collected information. Users must be notified if providing their information is voluntary or mandatory, and the effects, if any, of not providing all or any portion of the requested information.

2. Consent to Information Collection and Sharing

a. The privacy statement must inform visitors how they grant consent for the use of information they provide on the Web site.

3. Privacy Rights

a. The privacy statement must inform visitors of their rights under the Privacy Act or other applicable privacy laws.

4. Collection of Personally Identifiable Information

a. Informs visitors if collected information is maintained or retrieved by a personal identifier in a privacy system of records.

5. Automatically Collected Information

a. Web sites must inform visitors what information is gathered automatically (e.g., user IP address, location, time of visit), and for what purpose the information is gathered (e.g., site management, security).

6. Tracking Technology

a. Privacy law specifically targets the use of Internet tracking technology, also known as “cookies”.

i. Use of persistent cookies is prohibited, unless specifically approved by the Administrator of USAID.

ii. USAID must report any use of persistent cookies to OMB.

iii. Cookies used only to facilitate a Web site visitor's activity for a single session (session cookies) are permitted.

iv. Customizing features for Web site visitors is permitted with the Administrator's approval, but the Privacy Act statement must be clearly stated on the Web site.

v. Password access without use of persistent cookies or other similar tracking technology is permitted.

7. Information Security

a. Use clear language to describe Agency practices of protecting information and safeguards used to identify and prevent attacks on the Web site's information and systems.

8. Interaction With Children

a. Any site that provides content to children under the age of 13 and collects PII from these visitors must incorporate requirements of the "Children's Online Privacy Protection Act" (COPPA) in its privacy policy.

9. Law Enforcement and Homeland Security Sharing

a. Where applicable, privacy policy may indicate the sharing of collected information for authorized law enforcement purposes.

10. Privacy Policy in Machine-Readable Formats

a. Federal agencies must provide technical mechanisms to translate privacy policy into a standardized machine-readable format.

USAID Systems Owners, or designated personnel or office, must monitor all USAID 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 sites until the deficiencies are corrected.

508.3.6.1 Public Web Sites

Effective Date: 08/31/2007

USAID's use of publicly facing Web sites creates new challenges for privacy protections while enabling greater dissemination or exchange of information via Internet technologies.

How and when information is collected from Web site visitors is not always obvious to the Web site visitor. Public Web sites officially sponsored by USAID or managed by contractors who design, maintain, or operate Web sites on behalf of USAID must

comply with applicable privacy laws specific to Federal public Web sites and this chapter.

1. LPA must report on the progress of implementing machine readability technologies associated with public-facing USAID Web sites.

2. LPA must verify that USAID privacy policy pages on publicly accessible Web sites contain programming code that enables accessibility devices to automatically read Web site content.

*508.3.6.2 Third-Party Web Sites

Effective Date: 06/25/2010

*This section addresses the USAID policy for when third-party Web sites or applications are developed and/or implemented on behalf of the Agency. The policy requirements contained within this section are specifically derived from **OMB M10-23, Guidance for Agency Use of Third-Party Websites and Applications** or as amended. By USAID abiding by the requirements contained within **OMB 10-23** the protection of PII data elements maintained by USAID is enhanced. USAID business or system owners must comply with this policy in conjunction with **The Privacy Act of 1974** and all applicable laws when implementing third-party Web site offerings or services.

508.3.7 Access and Amendment Requests

Effective Date: 08/31/2007

Under the Privacy Act, U.S. citizens and legal aliens may request access to records about themselves to view or amend their information. The Privacy Office must establish and implement adequate means to track and report privacy requests. This requires maintaining records detailing to whom, what, why, and when PII was requested and disclosed by request, for purposes other than USAID routine uses identified in the Federal Register. This requirement applies to both manual and automated records. Reports of such requests must be provided to the CPO upon request, but not less than annually for end of fiscal year reporting. The PAIO must process Privacy Act inquiries and requests. The CPO must arbitrate escalated privacy requests with the assistance of the Office of the General Counsel.

A proper Privacy Act request is one in which the individual seeks to access or amend his or her records from within a system of records. Individuals who request access to or amendment of their PII must submit the request in writing. Each request must contain as much detail as possible to identify the information requested or sought to be amended. The request must contain the requestor's signature and proof of the individual's identity.

If the requestor is not the individual about whom the information pertains, written consent of the individual is required. The parent of any minor, or the legal guardian of any individual who has been declared incompetent, due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

Persons who are not U.S. citizens may use the provisions of the **Freedom of Information Act** to request information. See **ADS 507, Freedom of Information Act (FOIA),** for additional guidance.

To make a Privacy Act request, requestors must send a written request via the U.S. Postal Service or commercial service to the following address:

United States Agency for International Development
Office of the Chief Privacy Officer
Privacy Act Requests
Potomac Yards Two
2733 South Crystal Drive
11th Floor, Room 11114
Arlington, VA 22202

Requestors may use the **USAID Privacy Request Form.** Please contact **privacy@usaid.gov** for a copy of that form as a guide for creating this request. This form must be posted on the USAID public Web site for the public to download.

[Please Note: This document is only available on the USAID Intranet.]

508.3.7.1 Amending Records

Effective Date: 08/31/2007

Individuals may request amendments of records pertaining to them. The request must be in writing. Once USAID receives a receipt of a request to amend a record, the Privacy Office must provide a written acknowledgement within 10 business days and promptly either

1. Make any correction of any portion which the individual believes is not accurate, relevant, timely, or complete; or

2. Inform the individual of its refusal to amend the record as requested, provide the reason for the refusal, and provide information on USAID procedures for the individual to request a review of the refusal.

Additional requirements for record amendment include the following action:

1. For all requests, USAID must respond to a request for review within 30 business days from the date the written request is submitted, unless the Administrator extends the 30-day period.

Exceptions to the normal review response may result in USAID's refusal to provide requested records. Excepted actions include the following:

1. After the Agency has completed its review, if the reviewing official refuses

to amend the record in accordance with the request, USAID must:

a. Permit the individual to file with the Agency a concise statement giving the reasons for their disagreement with the refusal of the Agency; and

b. Notify the individual of the provisions for judicial review of the reviewing official's determination.

2. When a record is not amended and the individual files a statement of disagreement, USAID must do the following for any disclosure occurring after the filing of the statement:

a. Clearly note any portion of the record which is disputed, and

b. Provide copies of the statement of disagreement.

508.3.7.2 Rules for Disclosure

Effective Date: 08/31/2007

USAID must not disclose any record contained in a system of records by any means of communication to any person, except by written request or prior written consent of~~,~~ the individual to whom the record pertains. See **5 USC 552a(b)(1)-(12)** for the twelve specific exceptions to the “No Disclosure Without Consent Rule” **(OMB M-07-16).**

508.3.7.3 Disclosure Exemptions

Effective Date: 08/31/2007

Under certain circumstances, the Privacy Act protects information that may be exempt from disclosure. The USAID Administrator must include in the statement (required under **5 USC Section 553**, on rulemaking) the reasons why the system of records is exempt from such disclosure rules. See **5 USC section 552a(d)(5)** for Special Exemptions, **5 USC 552a (j)** for General Exemptions and **USC 552a(k)(1)(7)** for Specific Exemptions.

508.3.7.4 Disclosure Accounting

Effective Date: 08/31/2007

USAID must maintain accounting of privacy records under its control. Except for routine intra-agency or FOIA disclosures, accounting for each requested record must include the following:

1. Date, nature, and purpose of each disclosure of a record to any person or agency;

2. Name and address of the person or agency to whom the disclosure was made;

3. Retaining account of a disclosure for a minimum of five years, or the life or the record, whichever is longer;

4. Accounting of disclosures available to individuals named in the record at his or her request (except for disclosures made as a part of law enforcement activity); and

5. Informing any person or other agency about any correction or notation of dispute made by USAID of any record that has been disclosed to an individual or agency, if an accounting of that disclosure is made.

508.3.7.5 Appeals Process

Effective Date: 08/31/2007

A requester has the right to file an administrative appeal if an adverse determination is made. See **5 U.S.C. 552a(f)(4) Agency Rules**.

The Chief Privacy Officer will administer all appeals, in conjunction with the USAID Office of the General Counsel, or, where the system owner is the OIG, in conjunction with Legal Counsel to the OIG. All written inquiries must be sent to the following address:

United States Agency for International Development
Office of the Chief Privacy Officer
Privacy Act Requests - Appeals
Potomac Yards Two
2733 South Crystal Drive
11th Floor Room 11114
Arlington, VA 22202

If an individual requests an appeal, the requestor must provide the Office of the CPO with the following items:

- A letter describing the requested action, the resulting decision, and the reason for the appeal; and
- Copies of the original request and resulting decision.

The CPO will provide a written response to the requestor within 30 days with its final decision.

508.3.7.6 Civil Remedies and Criminal Penalties

Effective Date: 08/31/2007

Violation of the USAID Privacy Policy and the Privacy Act carries severe penalties for those who knowingly violate the law. See Chapter II – Agency for International

Development Part 215 – Regulations for Implementation of Privacy Act of 1974 (**22 CFR 215.12**) for specific civil remedies and criminal penalties.

508.3.8 Privacy Information Usage and Maintenance

Effective Date: 08/31/2007

All employees are responsible for proper usage of personally identifiable information. This includes maintaining the quality and integrity of records containing PII, data sharing, and the securing the systems on which PII resides. In accordance with **OMB M-07-16**, USAID systems, business owners, and processes must cease any superfluous collection and use of social security numbers.

508.3.8.1 Data Quality

Effective Date: 08/31/2007

USAID system of records owners 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.

508.3.8.2 Data Integrity Board

Effective Date: 08/31/2007

If USAID participates in or conducts matching programs, a Data Integrity Board must be established. The Data Integrity Board must review, approve, and maintain all written agreements for receipt or disclosure of Agency records for matching programs. This assures compliance with all relevant statutes, regulations, and guidelines. See **5 U.S.C. 552a(u), Data Integrity Boards**.

508.3.8.3 Matching Programs and Agreements

Effective Date: 08/31/2007

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.

USAID staff must not disclose any records contained in a SOR to a recipient agency or non-Federal agency for use in a computer matching program, except in compliance with a written agreement between USAID, as the source agency, and the recipient agency or non-Federal agency.

See **5 U.S.C. 552a(o), Matching Agreements**.

508.3.9 Privacy Systems and Information Security

Effective Date: 08/31/2007

USAID SORs owners must establish appropriate administrative, technical, and physical safeguards for SORs. Those safeguards will ensure the security, integrity, and

confidentiality of privacy records contained in the SORs, in accordance with Federal Information Security Management Act (FISMA) requirements and the Privacy Act.

1. System owners must review the type of information stored, processed, transmitted on the system, and determine the system security categorization.

2. A system security plan is required because personally identifiable information requires additional safeguards. The system security plan must detail the management, operational, and technical controls that protect PII on the system.

3. USAID staff must not remove, transport, or store personally identifiable information (PII) to include email transmissions or using any form of electronic media, including government furnished equipment, if the media cannot be encrypted using a FIPS 140-2 approved encryption algorithm. (**OMB M06-06**)

a. If the personally identifiable information is to be physically transported beyond the USAID security perimeter, the Chief Information Security Officer or System ISSO must authorize all deviations from this policy. (**OMB M06-16**)

4. The System Owner (SO) must authorize, in writing, any remote access, transportation or storage of personally identifiable information.

a. SO(s) must ensure that all remote access sessions to the applicable system does not allow for the downloading of PII data or the storage of such data by remote users. (**OMB M06-06**)

b. If the remote storage of PII or SBU data is allowed, SO(s) must implement **NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations** (PL-4, SC-4, and SC-13), ensuring that information is stored only in encrypted form. (**OMB M06-06**) Additional USAID guidance is provided in **ADS 545**.

5. Staff must provide written justification to the System Owner for any request to remotely access, transport, or store personally identifiable information. If authorized by the System Owner, staff must safeguard the data removed or accessed remotely using security controls approved within the system certification and accreditation.

508.3.9.1 Security Controls for PII

Effective Date: 08/31/2007

Personally identifiable information (PII) is considered Sensitive But Unclassified (SBU) and is subject to USAID security policy associated with SBU systems and data. With this SBU distinction, additional controls must be applied to protect that type of

information. When USAID PII data is physically transported outside of the Agency's secured, physical perimeters (this includes information transported on removable media and on portable and mobile devices such as laptop computers, universal serial bus (USB) storage drives, and personal digital assistants (PDA)) it must be encrypted using a FIPS 140-2 approved algorithm as defined by the National Institute of Standards and Technology (NIST). (**OMB M06-06)**

USAID SO(s) must verify information categorization to ensure identification of personally identifiable information requiring protection when accessed remotely or physically removed. The guidance for this information categorization is FIPS 199. The SO is to ensure all personally identifiable information through which a moderate or high impact might result has been explicitly identified.

SO must log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required (**OMB M06-06**).

All USAID mobile computing devices must use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity. (**OMB M-07-16**)

Security controls include mandatory Certification and Accreditation (C&A) of systems that contain PII. **ADS 545** establishes policy requirements on system Certification and Accreditation.

508.3.9.2 Transmission and Transport of PII

Effective Date: 08/31/2007

This section addresses USAID regulations specifying requirements for transmission and transport of PII. **OMB M06-06** requires that mobile computers, devices, personal digital assistants, etc. that carry SBU or greater classified information, as designated by the A/AID, must encrypt all data. USAID privacy policy requirements for the transmission and transportation of PII data is as follows:

1. PII may be sent via the U.S. Postal Service, Army Post Office (APO), commercial messenger, or unclassified registered pouch.

2. Regardless of method, transmission of PII should be made through means that limit the potential for unauthorized disclosure.

3. PII custodians should consider the destination and medium of transmission to determine whether specific information warrants a higher level of protection accorded by a secure fax, phone, or other encrypted means of communication.

a. Refer to **ADS 545**, for policy directives and required procedures on encryption.

4. System Owners must authorize remote access of PII.

5. USAID staffers who must process PII remotely must only access PII via the USAID Server Based Computing (SBC) process. This process requires the use of two-factor authentication, where one of the factors is a secure remote access token or device that is separate from the computing device (**OMB M06-06**).

a. Remote access must only be allowed through USAID virtual private network (VPN) sessions authenticated with authorized USAID security tokens or applicable USAID sanctioned X.509v3 digital credentials and NIST SP 800-53(a) or greater control AC-17. (**OMB M06-06**)

b. USAID remote access sessions and mobile devices must use a "time-out" function requiring user re-authentication after 30 minutes inactivity (**OMB M06-06**).

6. PII data must not be downloaded to any device or media (e.g., USAID-issued laptops, home computers, personal digital assistants (PDAs), or any other portable storage media) when accessed via USAID sanctioned Virtual Private Network (VPN) connections using secure remote authentication tokens (**OMB M06-06**).

Contact the Office of the CPO at **privacy@usaid.gov** for questions concerning the proper transmission protections for PII data elements.

508.3.9.3 Storage and Destruction of PII

Effective Date: 08/31/2007

PII custodians must carefully store and destroy media containing PII by approved methods.

1. During non-duty hours, documents or media containing PII must be secured within a locked office or suite, or secured in locked containers such as a file cabinet;

2. Destroy PII documents by pulverizing, incineration, abrasion, shredding or acid; or

3. USAID must store and destroy media containing PII in accordance with methods described in **USAID Media Handling Procedures and Guidelines, Section 9**.

Further discussion of privacy policy for media storage and destruction is outside the scope of **ADS 508**, but is provided in **ADS 545**.

508.3.9.4 Rules of Conduct

Effective Date: 08/31/2007

USAID System Owners have established rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records under their responsibility. SOR rules of conduct must be signed by the system users and maintained as system records by the System Owner (**OMB M-07-16**). See USAID **Rules of Behavior** for additional guidance) System Owners must validate the following:

1. Each person granted access to the system is trained in his or her responsibilities for privacy information on the system,

2. Each system user safeguards PII within his or her specific responsibility,

3. Each user of the SOR complies with USAID policy and Federal rules and requirements associated with SORs,

4. Each user acknowledges the penalties for non-compliance with adopted rules and procedures associated with privacy systems, and

5. All users and supervisors with authorized access to PII must sign a document that clearly describes their responsibilities for each system they are authorized to access. This action must be done annually or when access permissions change for any system.

508.3.9.5 Incident Reporting

Effective Date: 08/31/2007

Incidents involving a security breach of PII have a very critical time-period for reporting. Using the reporting process defined in **ADS 545**, users must immediately report all security incidents involving PII or suspected breaches of PII security to the Chief Information Security Officer (CISO). The CISO must then report the incident to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery or detection. (**OMB M-07-16**)

508.3.10 Privacy Breach

Effective Date: 08/31/2007

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 both electronic systems as well as paper documents. In short, agencies are required to report on the security of information systems in any formant (e.g., paper, electronic, etc.). In addition, an effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to person 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. (**OMB M-07-16**).

- Examples of these PII breaches include lost or stolen laptops containing personally identifiable information or mistakenly sending an unencrypted e-mail containing PII to the wrong person;

- For breaches involving government-authorized credit cards, the issuing bank must be notified in accordance with US-CERT directions. (**OMB M-07-16**).

USAID personnel and contractors are responsible for reporting possible privacy breaches to the USAID CPO as outlined in **USAID External Breach Notification Process and Procedures**.

*[Please Note: This document is only available on the USAID Intranet. Please contact **privacy@usaid.gov** for a copy.]*

In accordance with **OMB M-07-16**, the likely risk of harm and the level of impact will determine when, what, how and to whom notification must be given. The "openness principle" of the Privacy Act requires USAID System Owners to inform individuals about how their information is being accessed and used, and may help individuals mitigate the potential harms resulting from a breach.

In accordance with **OMB M-07-16**, five factors should be considered to assess the likely risk of harm related to PII data element breaches.

If confirmed, the CPO's office will perform further analysis to assess the level of risk associated by the breach, determine the escalation level, and provide recommendations to the Breach Response Team.

The USAID Chief Information Officer, in conjunction with the USAID CPO, has developed a breach notification policy and plan. Approved processes, procedures, and templates are provided in the External Breach Notification Process and Procedures. In implementing the policy and plan, the USAID Administrator will make final decisions regarding breach notification.

The USAID Administrator established a Breach Response Team whose members include the Chief Information Officer (CIO), Chief Privacy Officer (CPO), Senior Agency Official for Privacy (SAOP), Communications Office, Legislative and Public Affairs Office (LPA), General Counsel (GC), and the USAID office that has responsibility for budget and procurement functions. (**OMB M-07-16**).

*[Please Note: The breach notification policy and plan documents are only available on the USAID Intranet. Please contact **privacy@usaid.gov** to request a copy.]*

508.3.11 Privacy Reporting and Notifications

Effective Date: 08/31/2007

OMB evaluates the USAID Privacy Policy and its program at the end of each fiscal year, based on reporting provided about each element of USAID's program. OMB provides instructions for agency reporting under the Federal Information Security Management Act (FISMA). FISMA and privacy provisions of the E-Government Act emphasize incorporation of security and new technologies as part of robust privacy programs. Updated reporting instructions in **OMB M-06-20** and **OMB M-07-16** provide reporting formats for each responsible Agency officer. USAID must report as listed below:

1. System of Records and System of Records Notices (SORNs);

2. Privacy awareness training;

3. Web privacy policies;

4. Use of persistent tracking technology, safeguards used to protect information collected, use approval by the agency official, and actual privacy policy notification of its use;

5. Internal oversight controls;

6. Security safeguards implemented for privacy systems (, Web sites, other databases) as defined in USAID Security Certification and Accreditation requirements, and in alignment with National Institutes of Standards and Technology standards and guidelines;

7. Contact information for officials principally responsible for IT, Web, and privacy matters, to include name and title;

8. Complete inventory of Agency information systems;

9. Results of Senior Agency Official review of how USAID safeguards personally identifiable information;

10. Identify any physical or electronic incidents involving the loss of or unauthorized access to personally identifiable information and report them in accordance with policies outlined in **OMB Memorandum M-06-19** and **OMB M-07-16**;

11. Develop and make public a schedule for USAID to use to periodically update the review of its PII holdings. This schedule may become part of the Agency's annual review of Privacy Act system of records notices; and

12. Report annually to OMB and Congress on the effectiveness of USAID's Privacy Program.

508.3.12 Privacy Documentation Process
Effective Date: 08/31/2007

The Publications Officer is responsible for submitting required Privacy documentation to the Federal Register. The privacy documentation process is a lengthy one, for which System Owners must plan adequate time. Documentation submitted by the Publications Officer includes System of Records Notices (SORNs), Information Collection Request (ICR) notices, and Freedom of Information Act (FOIA) notices.

The Publications Officer, through the Privacy Office, must publish in the Federal Register a notice of establishment or revision of any matching program with a non-Federal agency. This notice must be published 30 days prior to such a program's operation.

See **Filing a System of Records Notice**, and **Information Collection Request Process and Procedures**, and **ADS 507** for details about these requirements.

508.3.13 Federal Legislation Related to the Privacy Act
Effective Date: 08/31/2007

"Companion" laws related to the Privacy Act have potential implications for USAID systems. Such implications may include the following:

1. The amount of time required to put a new system into production,
2. The cost and expertise required to implement security controls to protect PII, and
3. Possible denial of permission to use the system as designed.

*508.4 MANDATORY REFERENCES
Effective Date: 06/25/2010

*508.4.1 External Mandatory References
Effective Date: 06/25/2010

These references are linked to the actual document from the originating source to ensure accuracy of data.

a. **The Privacy Act of 1974 (Public Law 93-579, 5 USC Section 552a, as Amended)**

b. **E-Government Act of 2002 Section 208 (Public Law 107-347, 44 USC Ch. 36), Dec.17, 2002**

c. **The Computer Matching and Privacy Protection Act (CMPPA) of 1988 (Public Law 100-503)**

d. The Computer Matching and Privacy Protection Amendments of 1990 (Public Law 101-508)

e. Federal Information Security Management Act of 2002, (Title III of the E-Government Act of 2002), December 2002, as amended

f. Paperwork Reduction Act of 1995 (Public Law 104-13) May 22, 1995

g. Children's Online Privacy Protection Act of 1998

h. Government Paperwork Elimination Act (Public Law 105-277, Title XVII), as amended, October 21, 1998

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

j. Consolidated Appropriations Act 2005 (H.R. 4818), signed December 8, 2004

k. U.S. Code, Title 5, Part 1, Chapter 5, Subchapter II, section 553, Rule making

l. 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

m. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 23, 2003

n. OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, December 17, 2004

o. OMB Memorandum 05-15, Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, June 13, 2005

p. OMB Memorandum 06-15, Safeguarding Personally Identifiable Information, May 22, 2006

q. OMB Memorandum 06-16, Protection of Sensitive Agency Information, June 23, 2006

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

s. OMB Memorandum 06-20, FY2006 Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management

t. OMB FY 2007 Instructions for Preparing Federal Information Security Management Act Report and Privacy Management Report

u. Executive Order: Strengthening Federal Efforts to Protect Against Identity Theft

v. 5 USC 552a

w. 22 CFR 215

***x.** OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)

***y.** OMB Memorandum 10-06, Open Government Directive (December 8, 2009)

***z.** OMB Memorandum 10-22, Online Use of Web Measurement and Customization Technologies (June 25, 2010)

***aa.** OMB Memorandum 10-23, Agency Use of Third-Party Websites and Applications (June 25, 2010)

***ab.** 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d)

508.4.2 Internal Mandatory References

Effective Date: 08/31/2007

a. ADS 507, Freedom of Information Act

b. ADS 545, Information System Security

c. ADS 557, Public Information

d. 557mac, Updated Privacy Policy for USAID Information Technology Systems, Including Publicly Accessible Web sites, January 14, 2004

e. Privacy Impact Assessment Process and Procedures

f. Filing a System of Records Notice Process and Procedures

***g.** 508mad, Common Sense and Ad Hoc Requests

508.4.3 Mandatory Forms

Effective Date: 08/31/2007

a. USAID Information Collection Request Process and Procedures

b. USAID Privacy Request Form – USAID Form 508-PR-06v1 [Note: This document is only available on the USAID Intranet. Please contact privacy@usaid.gov if you need a copy.]

c. Privacy Impact Assessment Form, Revision 3, April 2007

d. OMB Form 83-I, Paperwork Reduction Act Submission, October 1995

e. USAID System of Records Notice Template, Version 2.0, October 2006

508.4 Additional Help

Effective Date: 08/31/2007

a. Privacy Basics

508.5 DEFINITIONS

Effective Date: 08/31/2007

The terms and definitions below were added into the ADS glossary.

Access to information
Giving members of the public, at their request, information to which they are entitled by a law such as the Privacy Act or FOIA. (Chapter 508)

Chief Privacy Officer (CPO)
The individual who has overall Agency responsibility for policy development, oversight, and implementation of an agency-wide privacy program. (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)

Encryption
This is the act of transforming information into an unintelligible form, specifically to obscure its meaning or content. (Chapters 508, **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)

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
Information in an IT system or online collection: 1) that directly identifies an individual (e.g., name, address, social security number, or other identifying number or code, telephone number, e-mail address, etc.) or 2) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). (Chapter 508)

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. {Source: a variation of a term from NSTISSI 4009} (Chapters **502**, 508, **545**, **552**, **562**, **620**)

Maintenance of PII
Collection, use, sharing, disclosure, transfer, and storage of personally identifiable information. (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)

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

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

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

Personally Identifiable Information
Information that directly identifies an individual. PII examples include name, address, social security number, 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. Same as "*information in an identifiable form".* (Chapter 508)

PII Custodian
Any USAID staff member who handles PII in the routine execution of daily work responsibilities. (Chapter 508)

Privacy Act record
Any item, collection, or grouping of information about an individual that is maintained in a system of records, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the name, or identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voiceprint 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 appearing on a Web site or information collection form the notifies 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. (Chapter 508)

Privacy Impact Assessment
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)

Privacy Policy In Standardized Machine-Readable Format
A statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a Web browser. (Chapter 508)

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
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 voiceprint or a photograph. (Chapter 508)

Responsible Official
The official having custody of the records requested, or a designated official, who makes initial determinations whether to grant or deny requests for notification, access to records, accounting of disclosures, and amendments of records. (Chapter 508)

Routine Use
Regarding disclosure of a record - usage of a record for a purpose which is compatible with the purpose for which it was collected. (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)

System Manager
The official identified in the system notice who is responsible for the operation and management of the system of records. (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, **545**)

System of records
A group of any records under the control of USAID from which information is retrieved by name, Social Security number, or other identifying symbol assigned to an individual. (Chapter 508)

508_032112