ADS Chapter 508

USAID Privacy Program

Revision Date: 08/31/2007
Responsible Office: M/CIO
File Name: 508_083107_cd49

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

**** This chapter has been revised in its entirety.***

Table of Contents

508.1 OVERVIEW 4

508.2 PRIMARY RESPONSIBILITIES 4

508.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES 5

508.3.1 Privacy Program Roles & Responsibilities 5

508.3.2 Privacy Act Awareness Training 8

508.3.3 Privacy Impact Assessments 8

508.3.4 Information Collection Requests 9
508.3.4.1 Preparing Paperwork Reduction Act Submission Worksheets 10

508.3.5 System of Records 11

508.3.6 Public Web Sites 13

508.3.7 Web Privacy Policies 13

508.3.8 Access and Amendment Requests 15
508.3.8.1 Amending Records 16
508.3.8.2 Rules for Disclosure 17
508.3.8.3 Disclosure Exemptions 17
508.3.8.4 Disclosure Accounting 17
508.3.8.5 Appeals Process 18
508.3.8.6 Civil Remedies and Criminal Penalties 18

508.3.9 Privacy Information Usage and Maintenance 19
508.3.9.1 Data Quality 19
508.3.9.2 Data Integrity Board 19
508.3.9.3 Matching Programs and Agreements 19

508.3.10 Privacy Systems and Information Security 19
508.3.10.1 Security Controls for PII 20
508.3.10.2 Transmission and Transport of PII 20
508.3.10.3 Storage and Destruction of PII 21

508.3.10.4 Rules of Conduct 21
508.3.10.5 Incident Reporting 22

508.3.11 Privacy Breach 22

508.3.12 Privacy Act Reporting and Notifications 23

508.3.13 Privacy Documentation Process 24

508.3.14 Federal Legislation Related to the Privacy Act 24

508.4 MANDATORY REFERENCES 25

508.4.1 External Mandatory References 25

508.4.2 Internal Mandatory References 26

508.4.3 Mandatory Forms 27

508.5 ADDITIONAL HELP 27

508.6 DEFINITIONS 27

ADS 508 – USAID Privacy Program

508.1 OVERVIEW

Effective date: 08/31/2007

The Privacy Act is a Federal law which mandates that Federal agencies protect personally identifiable information (PII) that they collect, maintain, or disseminate. The Privacy Act and subsequent statutory and regulatory guidance, listed in Section 508.3, establish specific requirements for the protection of PII within Federal information systems. This chapter defines the USAID Privacy Program, the roles and responsibilities within the program, and the policy directives and required procedures that establish the program's foundation. (See **Privacy Basics**, for additional guidance.)

508.2 PRIMARY RESPONSIBILITIES

Effective date: 08/31/2007

All USAID employees must protect personally identifiable information. The Privacy Act and subsequent statutory and regulatory guidance establish privacy-specific roles and responsibilities, which are described below.

a. The **Administrator (A/AID)** is responsible for establishing a Federally compliant Privacy Program that aligns with Federal law and the Office of Management and Budget (OMB) guidance.

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

c. The **Privacy Act Implementation Officer (PAIO)** serves as the principal contact for all day-to-day privacy program operations and implements privacy plans and procedures.

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

e. The **Office of the General Counsel (GC)** provides assistance as required by the Chief Privacy Officer (CPO), in review of reports, systems of records notices, proposed rules, and other related matters that are submitted to Congress, OMB, and other parties.

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

g. The **System Owners (SOs)** have numerous responsibilities for systems that contain PII. These responsibilities are described throughout this chapter. (See **508.3.1**)

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

508.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective date: 08/31/2007

USAID must establish and implement a Privacy Program that aligns with current Federal law, OMB guidance, and USAID management directives. The Program must meet the privacy reporting requirements and be sufficient to ensure the protection of personally identifiable information entrusted to the Agency.

508.3.1 Privacy Program Roles & Responsibilities

Effective date: 08/31/2007

a. The **Administrator (A/AID)** must

1. Delegate a Chief Privacy Officer with agency-wide program oversight and authority;
2. Implement an effective privacy management structure and develop a fully integrated Privacy Program, which demonstrates the priority of privacy;
3. Ensure that annual general privacy awareness training has been provided to all staff who maintain PII in routine performance of their jobs, and role-based training for individuals who have additional responsibility for PII;
4. Identify and report to OMB the senior official(s) primarily responsible for coordinating and implementing information technology, Web policies, and privacy policies;
5. Be made aware of the identity of individuals who have day-to-day responsibilities to implement privacy policy;
6. Designate reviewing officials for Privacy Impact Assessments (PIAs); and
7. Establish an Agency Breach Response Team.

b. The **Chief Privacy Officer (CPO)** must

1. Maintain oversight of the Privacy Program in compliance with all applicable statutory and regulatory guidance;

2. Establish and enforce privacy policy, which includes developing and disseminating privacy policies, plans, and procedures;

3. Implement and sustain Agency-wide technical safeguards for the use, collection, sharing, transfer, storage, and disclosure of privacy information;

4. Maintain appropriate documentation of privacy information (System of Records Notices, Privacy Impact Assessments, etc.);

5. Maintain data quality in privacy documentation;

6. Conduct continuous audits and periodic reviews to identify deficiencies, weaknesses, or risks;

7. Establish education and training on privacy and data protection policies, and evaluate them annually for compliance with statutory and regulatory guidance;

8. Evaluate annually the effectiveness of the procedure for conducting PIAs, and actively use the evaluation results to improve the procedure;

9. Evaluate legislative and regulatory proposals for collection, use, and disclosure of personal information by the Federal Government;

10. Prepare internal and external reports detailing Agency activities related to privacy, including complaints of privacy violations, implementation of section 552a of title 5 of United States Code, internal controls, and other relevant matters;

11. Arbitrate escalated privacy requests with assistance of the General Counsel;

12. Promptly, efficiently, and effectively implement policies to reduce information collection burdens on the public;

13. Review publications and forms, including

    - Publish Privacy Impact Assessments,
    - Create and publish System of Records Notices (SORNs),
    - Review and approve Information Collection Requests (ICRs) containing PII; and

14. Respond to all inquiries made during the consultative/review process with System Owners.

c. The **Privacy Act Implementation Officer (PAIO)** must

1. Assist System Owners in conducting PIAs;

2. Process Privacy Act inquiries and requests;

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

   - List all systems or information collections for which a PIA was made publicly available (posted on USAID Privacy page, Federal Register, or other site),

   - Maintain current list of principle Agency privacy contacts' names and titles for annual reporting; and

4. Maintain overall custodianship of protected records and data.

d. The USAID **Bureau of Legislative and Public Affairs (LPA)** must

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

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

   - Describe use of persistent cookies at USAID;

2. Report on the progress of implementing machine readability technology associated with public Web sites; and

3. Verify 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)** will carry out its statutory responsibilities pursuant to the Privacy Act, section 522 of the Consolidated Appropriations Act of 2005, and other statutory and regulatory guidance.

f. **System Owners** and managers for major and minor applications, general support systems, Web sites, databases, or other USAID systems that contain PII must

1. Verify that systems under their responsibility operate in compliance with Federal privacy laws and USAID privacy policy. This means conducting

privacy impact assessments (PIAs) on USAID systems and Web sites and filing a System of Records Notice (SORN), if applicable.

2. Revalidate PIAs annually, or revalidate PIAs when a significant change is made to the information system or the PII data elements collected, shared, or transmitted (maintained) by the information system.

3. Establish administrative, technical, and physical controls to store and safeguard records from unauthorized access or disclosure, and from physical damage or destruction; and

4. Conduct a Certification and Accreditation of any systems storing, processing, or transmitting PII to validate that appropriate security controls are applied and operate as intended. Information about the certification and accreditation process is provided in **ADS 545**, Information System Security.

508.3.2 Privacy Act Awareness Training

Effective date: 08/31/2007

The CPO must establish and provide annual Privacy Awareness training to all employees, particularly those who use PII in the routine performance of their jobs. USAID must provide targeted, role-based training to employees who are designated PII custodians and those who have greater responsibilities for PII.

Employees must complete this training to gain basic knowledge to maintain Privacy Act-protected information. If employees do not complete their annual privacy awareness training, the CPO may suspend their access to Privacy Act-protected information.

508.3.3 Privacy Impact Assessments

Effective date: 08/31/2007

Privacy Impact Assessments represent the process used to determine if USAID's information handling practices conform to the established legal, regulatory, and policy framework for privacy. Information handling practices include manual as well as automated processing. Conducting PIAs help System Owners to identify the following:

- Systems containing PII,
- Risks to PII that arise from electronic collection and maintenance of such data,
- Sharing of PII with other departments or agencies, and
- The physical security of the environment where PII is processed.

From this information, System Owners determine appropriate protections or alternative methods to mitigate identified risks.

System Owners must conduct or update a PIA under the following circumstances:

- For every electronic information system and information collection system (Privacy Office staff will assist System Owners in this process.);
- Before developing or procuring IT systems, or prior to initiating a new electronic collection of information for ten or more persons (excluding agencies or employees of the Federal Government);
- When a system change creates a new privacy risk;
- When information collection authorities, business processes, or other factors affecting the collection and handling of PII change; and
- Every three years for existing systems without changes.

The Privacy Office staff must review and clear each PIA.

- When the Privacy Office staff reviews and clears a PIA, they must notify the System Owner that the system has met its PIA requirements, and they must publish the PIA on USAID's public Web site.
- If the Privacy Office staff reviews but does not clear a PIA, they must notify the System Owner that the system has not met its PIA requirements and that the PIA process must be successfully completed. A PIA must be completed before the system is permitted to become operational.

System Owners must conduct their PIA using the template provided by the Privacy Office which may be downloaded from the Privacy Program Web page on the intranet or requested from **privacy@usaid.gov**. Privacy Office staff will assist System Owners in conducting PIAs. See **Privacy Impact Assessment (PIA) Process and Procedures** for additional guidance.

508.3.4 Information Collection Requests

Effective date: 08/31/2007

The Paperwork Reduction Act (PRA) and subsequent regulatory guidance establish requirements for information collection requests (ICRs). Surveys, questionnaires, registration forms, Web sites, and databases may represent information collection requests. If so, they are subject to the PRA.

ICRs are also subject to the Privacy Act when they include PII. If the information collection includes PII records maintained by USAID, then such a group of records

constitutes a system of records, which requires System Owners to publish a System of Records Notice (SORN) in the Federal Register. (See **Section 508.3.5** for details on System of Records.)

All ICR's must be cleared by the CPO staff to determine if a privacy impact assessment is required.

508.3.4.1 Preparing Paperwork Reduction Act Submission Worksheets

Effective date: 08/31/2007

System Owners must prepare and submit the Paperwork Reduction Act Submission Worksheets to OMB for ICRs. M/AS/IRD will assist System Owners with this task. The PRA requires that the agency 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 this notice is published, agencies must have at least a draft survey instrument available for the public to review. Agencies should state in their ICRs whether any comments were received from the public, and the comments should be addressed in the ICR that is submitted to OMB.

When submitting the ICR to OMB, agencies are required to place a second notice in the *Federal Register,* allowing a 30-day public comment period and notifying the public that OMB approval is being sought and that comments may be submitted to OMB. This notice runs concurrent with the first 30 days of OMB review, and OMB has a total of 60 days after receipt of the ICR to make its decision. Therefore, agencies need to allow at least 120 days for consideration of initial public comments, the second public comment period and OMB review, plus additional time for preparation of the ICR, as well as time lags for publication of *Federal Register* notices.

At the end of OMB's ICR process, OMB issues a control number for the approved ICR. This number must be displayed as part of the collection request on either the electronic/paper form used to collect information or on the Web site page where information is collected.

If the answer to any of the following questions is yes, then a System Owner must work with the CPO staff to process an ICR:

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

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

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

4. Does the collection request PII?

M/AS/IRD must assist System Owners developing ICRs to reduce collection of information to only those data elements that are relevant to the function of the data collection. (See **Information Collection Request Process and Procedures**, for additional guidance.)

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 SOR has the following two key distinctions:

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

2. The Agency retrieves records about individuals by reference to a personal identifier, such as name or Social Security number.

For each SOR, USAID must

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

2. Publish 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 and unless the record is being used as a routine use.

For each system of records a System Owner maintains, 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. Prepare documentation for the Publications Officer to publish a notice in the *Federal Register*, when a SOR is established or revised;

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

5. Maintain records with accuracy, relevance, timeliness, and completeness to assure fairness to the individual of record;

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

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

8. Require persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record to sign a Rules of Behavior for each SOR to which they are granted access. Information about this process is provided in **ADS 545**.

SOR reporting requirements include the following:

- Providing details about the uses of the information in the files,
- Types of records maintained, and
- An accounting of inquiries and requests for access to the records.

System Owners must file a System of Records Notice (SORN) and must complete the entire Federal Register review period before the system will be permitted to operate in the production environment. Approved processes, procedures, and templates are provided in **Filing a System of Records Notice**.

System Owners must send documentation in support of a new SOR or significant alteration to an existing SOR to the Privacy Office. The Privacy Office staff will post a notice for the SOR in the Federal Register. Federal Register publication of SORNs provides an opportunity for interested persons to submit written data, views, or arguments to the Agency.

Modification of information usage in a system with a SORN requires updating the 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.

System Owners must send this documentation to the USAID Privacy Office in sufficient time for CPO staff review, within the 40-day notice period required by OMB prior to placing a SOR in operation. The Privacy Office must post a notice with the Federal Register at least 40 days prior to publication of the SORN. See **Filing a System of Records Notice** for details on this process and its procedures.

All privacy documentation must be in electronic format. System Owners must submit documentation via e-mail to privacy@usaid.gov. Alternately, they may mail electronic media containing privacy documentation to the following address:

United States Agency for International Development
Chief Privacy Officer
Ronald Reagan Building
1300 Pennsylvania Avenue, NW
Room 2.12-004
Washington, D.C. 20523-2701

System Owners may submit questions or comments about privacy impact assessments, the template, systems of records notices, and information collection procedures from the Privacy Office through privacy@usaid.gov.

508.3.6 Public Web Sites

Effective date: 08/31/2007

USAID's use of public Web sites creates new challenges for privacy while enabling greater dissemination or exchange of information via Web technology. How and when information is collected from Web site visitors is not always obvious. Public Web sites sponsored by USAID or the contractors who design, maintain, or operate Web sites on behalf of the Agency, must comply with privacy laws specific to Federal public Web sites.

LPA must report on the progress of implementing machine readability technology associated with public Web sites. LPA must verify that USAID privacy policy pages on publicly-accessible Web sites contain code that enables accessibility devices to automatically read the policy.

508.3.7 Web Privacy Policies

Effective date: 08/31/2007

Web privacy policies must comply with OMB privacy-related memoranda and include notice about the nature, purpose, use, and sharing of information on Federal Web sites. The following areas are requirements for all Federal Web sites. System Owners are responsible for compliance with these requirements for their Web sites:

1. **Prominently Display a Privacy Act Statement** – Notifies users of the authority for and the purpose and use of the collected information. Users must be notified

if providing this 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** – The privacy statement must inform visitors how they grant consent for the use of information they provide on the Web site.

3. **Privacy Rights** – The privacy statement must inform visitors of their rights under the Privacy Act or other privacy laws.

4. **Collection of Personally Identifiable Information** – Informs visitors if collected information is maintained or retrieved by a personal identifier in a privacy system of records.

5. **Automatically Collected Information** – 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** - Privacy law specifically targets use of Internet tracking technology, also known as "cookies".

    - Use of persistent cookies is prohibited unless specifically approved by the Administrator.

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

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

    - Use of customizing features for Web site visitors is permitted with Administrator approval, but the Privacy Act statement must be clearly stated on the Web page.

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

7. **Information Security** – Use clear language to describe Agency practices of protecting information and safeguards used to identify and prevent attacks on the site's information and systems.

8. **Interaction With Children** – 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** – Where applicable, privacy policy may indicate the sharing of collected information for authorized law enforcement purposes.

10. **Privacy Policy in Machine-Readable Formats** – Federal agencies must provide technical mechanisms to translate privacy policy into a standardized machine-readable format.

USAID must monitor its external Web sites to ensure compliance with privacy requirements. The CPO may require corrective actions for sites determined to be non-compliant, and may shutdown sites until the deficiencies are corrected.

508.3.8 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 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 to be 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,** 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
Ronald Reagan Building
1300 Pennsylvania Ave., N.W
Room 2.12-004
Washington, DC 20523-2120

Requestors may use the **USAID Privacy Request Form [Note: This document is only available on the USAID Intranet. Please contact privacy@usaid.gov if you need a copy.]** as a guide for creating this request. This form must be posted on the USAID public Web site for the public to download.

For general questions about the Privacy Act request process, e-mail **privacy@usaid.gov**.

508.3.8.1 Amending Records

Effective date: 08/31/2007

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

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

- Inform the individual of its refusal to amend the record as requested and 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 actions:

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 refusal of the Agency to provide requested records. Excepted actions include the following:

- After the Agency has completed its review, if the reviewing official refuses to amend the record in accordance with the request, USAID must

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

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

- 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:

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

  - Provide copies of the statement of disagreement.

508.3.8.2 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 U.S.C. 552a** (b) (1) - (12) for exceptions to the "No Disclosure Without Consent Rule".

508.3.8.3 Disclosure Exemptions
Effective date: 08/31/2007

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

508.3.8.4 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:

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

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

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

- 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

- 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.

508.3.8.5 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**, as amended, (d) (2) Access to Records.

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
Ronald Reagan Building
1300 Pennsylvania Ave., N.W
Room 2.12-004
Washington, DC 20523-2120

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.

508.3.8.6 Civil Remedies and Criminal Penalties
Effective date: 08/31/2007

Violation of the USAID Privacy Program, and the Privacy Act on which it is founded, carries severe penalties for those who knowingly violate the law. See **22 CFR 215**.

508.3.9 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.

508.3.9.1 Data Quality
Effective date: 08/31/2007

USAID system of records owners must exercise due care in assuring 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.

508.3.9.2 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**, as amended, (u), Data Integrity Boards.

508.3.9.3 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**, as amended, (o), Matching Agreements.

508.3.10 Privacy Systems and Information Security
Effective date: 08/31/2007

USAID system of records owners must establish appropriate administrative, technical, and physical safeguards for SORs. This 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.

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

- 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.

- Staff must not remove, transport, or store personally identifiable information, to include email transmissions or using any form of electronic media, including government furnished equipment, if the media cannot be encrypted using FIPS 140-2 approved encryption, if the personally identifiable information is to be transported beyond the USAID security perimeter. The Chief Information Security Officer or System ISSO must authorize all deviations from this policy.

- The System Owner must authorize, in writing, any remote access, transportation, or storage of personally identifiable information.

- 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.

508.3.10.1 Security Controls for PII

Effective date: 08/31/2007

Personally identifiable information 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 the information. Additional controls include mandatory Certification and Accreditation of systems that contain PII. **ADS 545** establishes policy on system Certification and Accreditation. Additionally, information system security policy establishes restrictions on transmission, media transport, storage, and processing (e.g., telecommuting/off site) of SBU information.

508.3.10.2 Transmission and Transport of PII

Effective date: 08/31/2007

Regulations specify requirements for transmission and transport of PII, which include the following:

1. PII may be sent via the US Postal Service, Army Post Office, commercial messenger, or unclassified registered pouch.

2. Regardless of method, transmission of PII should be made through means which 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. Refer to **ADS 545**, for policy on encryption. Contact the Office of the CPO at **privacy@usaid.gov** for questions concerning proper transmission protections for PII.

4. System Owners must authorize remote access of PII.

5. USAID staffers who must process PII remotely, may only access PII via the Server Based Computing (SBC) process in place at USAID. This process uses two-factor authentication, where one of the factors is a secure remote access token.

6. PII accessed via secure remote token must not be downloaded to any device or media (e.g., USAID-issued laptops, home computers, or any portable storage media).

508.3.10.3 Storage and Destruction of PII
Effective date: 08/31/2007

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

- During non-duty hours, PII must be secured within a locked office or suite, or secured in a locked container such as a file cabinet.

- Destroy PII documents by shredding or burning.

- Media containing PII must be destroyed in accordance with methods described in **Media Handling Procedures and Guidelines**.

Further discussion of SBU policy is outside the scope of this ADS Chapter, but is provided in **ADS 545**.

508.3.10.4 Rules of Conduct
Effective date: 08/31/2007

USAID System Owners must establish 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. (See **Rules of Behavior** for additional guidance) System Owners must validate that

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

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

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

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

- 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 must be done annually or when access permissions change for any system.

508.3.10.5 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.

508.3.11 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. This includes lost or stolen laptops containing personally identifiable information or mistakenly sending an e-mail containing PII to the wrong person.

USAID personnel and contractors are responsible for reporting possible privacy breaches to the CPO as outlined in the **External Breach Notification Process and Procedures [Note: This document is only available on the USAID Intranet. Please contact privacy@usaid.gov if you need a copy.]**.

Every reported privacy breach will undergo a preliminary review by the CPO's Office to confirm a breach has occurred. If confirmed, the CPO's office will perform further analysis to assess the level of risk associated by the breach, escalation level and provide recommendations to the Breach Response Team.

The Administrator must establish a Breach Response Team including the Chief Information Officer, Chief Privacy Officer or Senior Agency Official for Privacy, Communications Office, Legislative Affairs Office, General Counsel and the Management Office which includes Budget and Procurement functions.

Chief Information Officer must develop a breach notification policy and plan. Approved processes, procedures, and templates are provided in **External Breach Notification Process and Procedures [Note: This document is only available on the USAID**

Intranet. Please contact privacy@usaid.gov if you need a copy.]. In implementing the policy and plan, the Administrator will make final decisions regarding breach notification.

508.3.12 Privacy Act Reporting and Notifications

Effective date: 08/31/2007

OMB evaluates the USAID Privacy 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** provide reporting formats for each responsible Agency officer. USAID must report on the following set of privacy and security elements in its Privacy Program:

CPO participation in the Agency Privacy Program;

Privacy Impact Assessments conducted for USAID IT systems or information collections;

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, the agency official approving this use, and actual privacy policy notification of its use;
5. Internal oversight controls;
6. Security safeguards implemented for privacy systems (system of records, 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. Implementation of machine-readable privacy tools, describing goals and progress toward achieving the end function;
8. Contact information for officials principally responsible for IT, Web, and privacy matters, to include name and title;
9. Complete inventory of agency information systems;
10. Results of Senior Agency Official review of how the Agency safeguards

personally identifiable information;

11. 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 06-19**;

12. Submit Privacy update reports quarterly with security updates to the President's Management Agenda scorecard. These updates are due on the first day of September, December, March, and June;

13. 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

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

508.3.13 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.)

508.3.14 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:

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

508.4 MANDATORY REFERENCES
Effective date: 08/31/2007

508.4.1 External Mandatory References
Effective date: 08/31/2007

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

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

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, § 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

508.4.2 Internal Mandatory References

Effective date: 08/31/2007

a. USAID Notice 7548, Updated Privacy Policy for USAID Information Technology Systems, Including Publicly Accessible Web Sites, January 14, 2004

b. ADS 507, Freedom of Information Act

c. ADS 545, Information System Security

d. ADS 557, Public Information

e. USAID/General Notice Policy, M/IRM 2/3/97 - *Sensitive But Unclassified (SBU)* Information Created, Processed, Stored, or Transmitted in Electronic Format, (REFERENCE: USAID/General Notice by IG/SEC dated 11/09/95)

f. Information Collection Request Process and Procedures

g. Privacy Impact Assessment Process and Procedures

h. Filing a System of Records Notice Process and Procedures

508.4.3 Mandatory Forms
Effective date: 08/31/2007

a. **USAID Information Collection Checklist, October 2006**

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**

508.5 ADDITIONAL HELP
Effective date: 08/31/2007

a. **Privacy Basics**

508.6 DEFINITIONS
Effective date: 08/31/2007

The terms and definitions below have been added into the ADS glossary. See the ADS Glossary for all terms and definitions.

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_083107_w092107_cd49