



USAID
FROM THE AMERICAN PEOPLE

Privacy Basics

An Additional Help Reference for
ADS Chapter 508

New Reference Date: 08/31/2007
Responsible Office: M/CIO
File Name: 508saa_083107_cd49

Privacy Basics

This additional help document answers basic questions about the Privacy Act and its application to USAID employees and contractors.

What is the Privacy Act?

The Privacy Act is a Federal Law. Its purpose is to balance the Government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy resulting from the collection, maintenance, use, and disclosure of their personal information.

The Privacy Act addresses how Federal agencies must protect personally identifiable information (PII) from unauthorized disclosure in both electronic and paper records, how the Federal Government must maintain and collect personal information, and to whom personal information can be disclosed.

The Act also permits an individual to gain access to most of their personal information that is maintained by Federal agencies and to seek amendment of any inaccurate, incomplete, untimely, or irrelevant information.

What is Personally Identifiable Information?

Personally Identifiable Information is any information about an individual maintained by an agency, including, but not limited to the following:

- Their name;
- Social security number;
- Date and place of birth;
- Mother's maiden name;
- Biometric records, etc., including any other personal information which is linked or linkable to an individual;
- Education;
- Financial transactions;
- Medical history; and
- Criminal or employment history and information which can be used to distinguish or trace an individual's identity.

Other examples of PII include address, 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, which, when taken together, can identify individuals.

Is PII Sensitive But Unclassified?

Yes, PII is considered Sensitive But Unclassified (SBU). Both SBU information and PII require greater controls against unauthorized disclosure and access than information that is unclassified. USAID staff must protect SBU information and PII against unauthorized access or disclosure based on a clearly demonstrated need to know or need to use basis. Failure to do so may result in administrative sanctions, and criminal and/or civil penalties.

For additional information on SBU information, contact the Chief Information Security Officer at ISSO@usaid.gov, or refer to [ADS 545](#), Information System Security.

To Whom Do the Privacy Act Provisions and Protections Apply?

All provisions and protections of the Privacy Act apply only to personally identifiable information maintained on individuals who are U.S. citizens and aliens who are lawfully admitted for permanent residence in the United States.

What Are the Responsibilities of Federal Employees and Contractors Under the Act?

All USAID employees and contractors must protect any personally identifiable information that they handle, process, compile, maintain, store, transmit, or report on in their daily work. [ADS 508, Section 508.2](#), Primary Responsibilities, details specific role-related privacy responsibilities.

How Must I Protect PII?

To protect PII, USAID staff must use proper collection, storage, transportation, transmission, and disposal methods, and must not disclose PII to unauthorized parties. **Section 508.3.8.10**, Privacy Systems and Information Security details these requirements.

What is a System Of Records?

A "system of records" is unique to the Privacy Act. The Act defines a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency that contains personally identifiable information. A "system of records" is a group of records from which information is actually

retrieved by name, Social Security number, or other identifying symbol assigned to an individual.

Who Must Comply with System Of Records Regulations?

Anyone, whether Federal employee or contractor, who maintains a system of records for the Federal Government must comply with the provisions and requirements of the Privacy Act and privacy provisions of the E-Government Act of 2002.

Examples of USAID personnel who may maintain systems of records include the following:

- System managers,
- Program managers,
- Personnel specialists,
- Finance officers,
- Investigators,
- Acquisition officials,
- Attorneys,
- Advisors, and
- Public affairs and disclosure officials.

Federal employees and contractors who fail to comply with provisions of the Privacy Act may be subject to administrative sanctions and subject to criminal and/or civil prosecution. Administrative sanctions are detailed in [ADS 508](#), **Section 508.3.6**, Civil Remedies and Criminal Penalties.

Which USAID Systems are Subject to the Privacy Act?

All USAID systems that contain personally identifiable information, in which the records are retrieved by a personally identifiable information data element, are subject to the Privacy Act. To determine if a system is subject to the Act, the System Owner must conduct a privacy impact assessment (PIA).

What is a Privacy Act Violation?

Violations include the following:

- Disclosure of PII contained in a system of record to unauthorized parties,
- Disclosure of PII without written consent of the individual to whom the record applies, and
- Unauthorized access to or modification of PII.

A “disclosure” can be by any means of communication – written, oral, electronic, or mechanical. For example, Social Security numbers are particularly sensitive and must never be disclosed to anyone who has no authorized business reason to have such information.

Exceptions to these rules are discussed in [ADS 508 Section 508.3.8.3](#) Disclosure Exemptions. USAID staff must report unauthorized PII disclosures immediately to the CPO’s office **(703) 666-1441**. Additionally, all reports of violations must be investigated and reported to OMB and Congress every two years in the Biennial Privacy Act Report.

What is Privacy Awareness Training and Who Must Take It?

Privacy awareness training provides all USAID staff with education on how to identify, protect, collect, maintain, and properly disseminate PII processed at USAID. USAID staff members who have privacy information-related responsibilities must attend role-based training. Privacy awareness training is mandatory and graded for Agency performance records. For questions about privacy training, contact the Chief Privacy Officer at privacy@usaid.gov.

508saa_083107_w092607_cd49