



USAID
FROM THE AMERICAN PEOPLE

USAID Privacy Threshold Analysis Template

A Mandatory Reference for ADS Chapter 508

New Reference: 03/07/2014
Responsible Office: M/CIO/IA
File Name: 508maj_030714



Management Bureau/Chief Information Officer/Information Assurance Division
(M/CIO/IA)

USAID PRIVACY THRESHOLD ANALYSIS (PTA)

[Click here to enter text.](#)

Version [Click here to enter text.](#)

Approved: [Click here to enter a date.](#)

3.2.2 About what types of people do you collect, use, maintain, or disseminate personal information?
<i>(Please check all that apply. If you choose Other, please provide the types of people.)</i>
<input type="checkbox"/> Citizens of the United States
<input type="checkbox"/> Aliens lawfully admitted to the United States for permanent residence
<input type="checkbox"/> USAID employees, including Foreign Service National (FSN) Direct Hires, FSN Personal Services Contractors, and Third Country National Employees
<input type="checkbox"/> Employees of USAID contractors or service providers
<input type="checkbox"/> Visitors to the United States
<input type="checkbox"/> Aliens
<input type="checkbox"/> Business Owners or Executives
<input type="checkbox"/> Others: Click here to enter text.
AP-1 Authority to Collect

3.2.3 What types of device, website, or platform related data associated with digital or mobile programs or services do you collect, use, maintain, or disseminate?
<i>(Please check all that apply. If you choose Other, please provide the types of data.)</i>
<input type="checkbox"/> Log Data (IP address, time, date, referrer site, browser type)
<input type="checkbox"/> Tracking Data (single- or multi-session cookies, beacons)
<input type="checkbox"/> Form Data
<input type="checkbox"/> User Names
<input type="checkbox"/> Passwords
<input type="checkbox"/> Unique Device Identifier
<input type="checkbox"/> Location or GPS Data
<input type="checkbox"/> Camera Controls (photo, video, videoconference)
<input type="checkbox"/> Microphone Controls
<input type="checkbox"/> Other Hardware or Software Controls
<input type="checkbox"/> Photo Data
<input type="checkbox"/> Audio or Sound Data
<input type="checkbox"/> Other Device Sensor Controls or Data

Click here to enter a date.

3.2.3 What types of device, website, or platform related data associated with digital or mobile programs or services do you collect, use, maintain, or disseminate?
<i>(Please check all that apply. If you choose Other, please provide the types of data.)</i>
<input type="checkbox"/> On/Off Status and Controls
<input type="checkbox"/> Cell Tower Records (logs, user location, time, date)
<input type="checkbox"/> Data Collected by Apps (itemize)
<input type="checkbox"/> Contact List and Directories
<input type="checkbox"/> Biometric Data or Related Data
<input type="checkbox"/> SD Card or Other Stored Data
<input type="checkbox"/> Network Status
<input type="checkbox"/> Network Communications Data
<input type="checkbox"/> Device Settings or Preferences (security, sharing, status)
<input type="checkbox"/> Other: Click here to enter text.
<input type="checkbox"/> None
AR-2 Privacy Impact and Risk Assessment SE-1 Inventory of Personally Identifiable Information

3.2.4 What PII, digital data, or mobile data <i>could be</i> made available to USAID or its contractors and service providers?
Click here to enter text.
<p>The use of third-party websites and applications, digital collaboration services, mobile services, and other new technologies can increase privacy risks significantly, because these technologies can make PII available even when USAID does not purposefully collect it.</p> <p>Describe the specific types of PII and data your technology makes available to USAID. Also, describe separately the specific types of PII and data your technology makes available to contractors and service providers. Please refer to Question 3.2.1 for specific types of PII and Question 3.2.2 for specific types of digital and mobile related data.</p> <p><i>Make PII available</i> includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the website or application. “Associate” can include activities commonly referred to as “friending,” “following,” “liking,” joining a “group,” becoming a “fan,” and comparable functions.</p>
DM-1 Minimization of Personally Identifiable Information

3.2.5 What are the authorities that permit you to collect, use, maintain, or disseminate PII and, specifically, Social Security Numbers (SSNs)?

Click here to enter text.

Please provide the name and citation for each statute, regulation, policy, and other authority (such as Executive Orders, OMB policies, NIST guidance) that authorize you to collect, use, maintain, and disseminate PII. Also include any Memoranda of Understanding (MOUs) that allow or require you to collect, use, maintain, and/or disseminate PII. Include also any internal USAID regulations, policies, memoranda, and other documents.

Please provide the name and citation for each statute, regulation, policy, and other authority that authorize you to collect, use, maintain, and disseminate SSNs, if you do so.

Describe how these authorities define the collection, use, maintenance, and dissemination of the PII or SSNs and relate to the program and system purpose.

AP-1 Authority to Collect

3.2.6 Who owns and/or controls the PII?

(Please check all that apply. Please provide the names of the specific organizations. If you choose Other, please provide the types of organizations and the name of each organization.)

USAID Office: Click here to enter text.

Another Federal Agency: Click here to enter text.

Contractor: Click here to enter text.

Cloud Computing Services Provider: Click here to enter text.

Third-Party Web Services Provider: Click here to enter text.

Mobile Services Provider: Click here to enter text.

Digital Collaboration Tools or Services Provider: Click here to enter text.

Other: Click here to enter text.

AR-3 Privacy Requirements for Contractors and Service Providers

UL-1 Internal Use

3.2.7 Who has access to the PII at USAID?

Click here to enter text.

Identify who within USAID, its contractors, and its service providers will have access to the PII. Describe what USAID offices and what types of USAID employees, contractors, and service providers have access to the PII. Also, include the level of access for each office and type of worker; that is, what PII to which they have access, the purpose of the access, and how they get access to the PII. Describe the procedures you use to determine which users may access the information and how you determine who has access.

Click here to enter a date.

3.2.7 Who has access to the PII at USAID?

UL-1 Internal Use

3.2.8 With whom do you share the PII outside of USAID? And whether (and how, if applicable) you will be using the system or related web site or application to engage with the public?

Click here to enter text.

Discuss the sharing of PII outside USAID. Identify the name of each system, person, or federal agency outside of USAID with whom you share PII, what PII you share, the purpose of the sharing, and how you share the PII (such as on a case-by-case basis, US mail, bulk transfer, or direct access).

Explain any use of the system or related web site or application that would make data assets available to the public, including 1) what data assets will be posted; 2) how the public will be able to interact with USAID; and 3) how the public will be able retrieve or use the data assets.

Person means any individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision.

UL-2 Information Sharing with Third Parties

3.3 SYSTEM INFORMATION

3.3.1 Describe the system and its purpose.

Click here to enter text.

Provide a general description of the system. The description should include the purpose of the system and how it supports the USAID program’s business function. Describe the way the system operates to achieve its purpose, how information is transmitted to and from the system, and any interconnections with other systems. Describe how the system will be used at USAID and provide information on where the system will be used, such as locally, stateside, overseas, or worldwide. Provide the system level, such as major application or general support system.

Examples of other information that should be included in the description, if applicable: New technology replacing a legacy system; system is a government-wide initiative or best practice; program is moving from a paper process to IT system; or the system has interdependencies on other systems.

The description should be as comprehensive as necessary to assist the public in understanding the system fully.

For this purpose, *system* means any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

AP-2 Purpose Specification

3.3.2 What type of system and/or technology is involved? <i>(Please check all that apply. If you choose New Technology or Other, please explain.)</i>
<input type="checkbox"/> Network
<input type="checkbox"/> Database
<input type="checkbox"/> Software
<input type="checkbox"/> Hardware
<input type="checkbox"/> Mobile Application or Platform
<input type="checkbox"/> Mobile Device Hardware (cameras, microphones, etc.)
<input type="checkbox"/> Quick Response (QR) Code (matrix geometric barcodes scanned by mobile devices)
<input type="checkbox"/> Wireless Network
<input type="checkbox"/> Social Media
<input type="checkbox"/> Advertising Platform
<input type="checkbox"/> Website or Webserver
<input type="checkbox"/> Web Application
<input type="checkbox"/> Third-Party Website or Application
<input type="checkbox"/> Geotagging (locational data embedded in photos and videos)
<input type="checkbox"/> Near Field Communications (NFC) (wireless communication where mobile devices connect without contact)
<input type="checkbox"/> Augmented Reality Devices (wearable computers, such as glasses or mobile devices, that augment perception)
<input type="checkbox"/> Facial Recognition
<input type="checkbox"/> Identity Authentication and Management
<input type="checkbox"/> Smart Grid
<input type="checkbox"/> Biometric Devices
<input type="checkbox"/> Bring Your Own Device (BYOD)
<input type="checkbox"/> Remote, Shared Data Storage and Processing (cloud computing services)
<input type="checkbox"/> Other: Click here to enter text.
<input type="checkbox"/> None
AR-2 Privacy Impact and Risk Assessment

3.3.3 What is the system status?
<i>(If this is an existing Information Collection, please enter the OMB Control Number. If you choose Other, please explain.)</i>
<input type="checkbox"/> New System Development or Procurement
<input type="checkbox"/> Existing System Being Updated
<input type="checkbox"/> Existing Information Collection OMB Control Number: Click here to enter text.
<input type="checkbox"/> New Data Collection Form or Survey
<input type="checkbox"/> Request for Dataset to be Published on an External Website
<input type="checkbox"/> Other: Click here to enter text.
AR-2 Privacy Impact and Risk Assessment

3.3.4 Do you use new technology or technology used in ways not previously used by USAID?
<i>(If you choose Yes, please provide the specifics of any new privacy risks and mitigation strategies.)</i>
<input type="checkbox"/> No.
<input type="checkbox"/> Yes: Click here to enter text.
Describe the new technology or the way you use technology that is new to USAID. Describe how such new technology or uses will affect the risks to the PII in the system.
AR-2 Privacy Impact and Risk Assessment

3.3.5 Who owns and/or controls the system involved?
<i>(Please check all that apply. Please provide the owners' and/or controllers' names for the items chosen.)</i>
<input type="checkbox"/> USAID Office: Click here to enter text.
<input type="checkbox"/> Another Federal Agency: Click here to enter text.
<input type="checkbox"/> Contractor: Click here to enter text.
<input type="checkbox"/> Cloud Computing Services Provider: Click here to enter text.
<input type="checkbox"/> Third-Party Website or Application Services Provider: Click here to enter text.
<input type="checkbox"/> Mobile Services Provider: Click here to enter text.
<input type="checkbox"/> Digital Collaboration Tools or Services Provider: Click here to enter text.
<input type="checkbox"/> Other: Click here to enter text.

3.3.5 Who owns and/or controls the system involved?

(Please check all that apply. Please provide the owners' and/or controllers' names for the items chosen.)

Cloud computing is remote, often shared, data storage and processing.

NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), three service models (Software as a Service, Platform as a Service, Infrastructure as a Service), and four deployment models (private cloud, community cloud, public cloud, hybrid cloud).

Third-party website or application means web-based technologies that are not exclusively operated or controlled by a government entity. Often these technologies are located on a “.com” website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency’s official website.

AR-3 Privacy Requirements for Contractors and Service Providers
UL-1 Internal Use

3.3.6 Who is involved in the development and/or continuing operation of the system and/or technology?

(Please check all that apply. Please provide the owners' and/or controllers' names for the items chosen.)

Mobile device manufacturer or other equipment manufacturer: Click here to enter text.

Application Developer: Click here to enter text.

Content Developer or Publisher: Click here to enter text.

Wireless Carrier: Click here to enter text.

Advertiser: Click here to enter text.

Equipment or Device Vendor: Click here to enter text.

Device User: Click here to enter text.

Internet Service Provider: Click here to enter text.

Third-Party Data Source (Data Broker): Click here to enter text.

Other: Click here to enter text.

AR-3 Privacy Requirements for Contractors and Service Providers
UL-1 Internal Use



Please stop here and send this form to the Privacy Office at privacy@usaid.gov. The Privacy Office will review your information and contact you.

Click here to enter a date.

- If more information is needed, the Privacy Office will contact you with questions or will send you the appropriate form(s) to complete.
- If this PTA is ready for the approval process, the Privacy Office will send you this form to sign.

SENSITIVE BUT UNCLASSIFIED

[Click here to enter text.](#) *Privacy Threshold Analysis*

ID	Privacy Controls
SE Security	Supplements the security controls in Appendix F to ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by USAID against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR Transparency	Ensures that USAID provides public notice of its information practices and the privacy impact of its programs and activities.
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL Use Limitation	Ensures that USAID only uses PII either as specified in its public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

[Click here to enter a date.](#)