USAID Privacy Impact Assessment Template

A Mandatory Reference for ADS Chapter 508

New Reference: 03/07/2014
Responsible Office: M/CIO/IA
File Name: 508mac_030714

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

PRIVACY IMPACT ASSESSMENT (PIA)

Click here to enter text.

Click here to enter text.

Version 1D

Approved: Click here to enter a date.

CHANGE HISTORY

The table below identifies all changes incorporated into this template. Baseline changes require review and approval. The version states the number with either D for draft or F for final.

Change #	Date	Version #	Description
1.	Click here to enter a date.	1D	Click here to enter text.
2.	Click here to enter a date.		Click here to enter text.
3.	Click here to enter a date.		Click here to enter text.
	Click here to enter a date.		Click here to enter text.
	Click here to enter a date.		Click here to enter text.

TABLE OF CONTENTS

1. INTRODUCTION

The USAID Privacy Office is using this Privacy Impact Assessment (PIA) Template to gather information from program managers, system owners, and information system security officers in order to analyze USAID information technology and information collections (systems) that collect, use, maintain, or disseminate personally identifiable information (PII).

The PIA process should accomplish two goals: 1) determine the privacy risks and effects of collecting, using, maintaining, and disseminating PII; and 2) evaluate and enforce protections and alternative processes for handling PII to reduce potential privacy risks to acceptable levels.

Type *Not Applicable* in the answer boxes for those questions that do not apply to your system and explain why the question is not applicable. Each section includes assistance (in blue text) on how to answer the question. For additional instructions on how to complete this PIA Template, please see Appendix C Conducting the PIA.

If you have questions about or would like assistance with this PIA Template, the PIA process, or other privacy compliance requirements please contact the USAID Privacy Office at **privacy@usaid.gov**.

2. CONTACT INFORMATION AND APPROVAL SIGNATURES

PROGRAM MANAGER

Name:
Title:
Office Name:
Office Phone #:
E-Mail:

SYSTEM OWNER

Name:
Title:
Office Name:
Office Phone #:
E-Mail:

Signature Date: Click here to enter a date.

Signature:

INFORMATION SYSTEM SECURITY OFFICER

Name:
Title:
Office Name:
Office Phone #:
E-Mail:

Signature Date: Click here to enter a date.

Signature:

PRIVACY ANALYST

Name:
Title:
Office Name: Privacy Office (M/CIO/IA/PO)
Office Phone #:
E-Mail:

Signature Date: Click here to enter a date.

Signature:

CHIEF PRIVACY OFFICER

Name: William Morgan
Title: Chief Privacy Officer
Office Name: Office of Information Assurance (M/CIO/IA)
Office Phone #: x65691
E-Mail: **wmorgan@usaid.gov**

Signature Date: Click here to enter a date.

Signature:

3. INFORMATION

3.1 PROGRAM INFORMATION

3.1.1 Describe the program and its purpose.

Click here to enter text.

Provide a general description of the program. The description should include the purpose of the program and how it supports a USAID business function. Describe the way the program operates to achieve its purpose, and any interconnections with other programs. Provide information on where the program operates, such as locally, stateside, overseas, or worldwide.

Describe the types of information that you use, and explain why and how you use the information.

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

AP-2 Purpose Specification

3.1.2 What types of paper documents, systems, electronic media, digital collaboration tools or services, and/or mobile services do you employ to collect, use, maintain, and disseminate information?

Click here to enter text.

Provide a general description of the paper documents, information systems, and/or electronic media that the program uses to meets its goals and objectives. The description should show who uses the information, how the information moves within the program, how information is transmitted to and from the program, and how the information is stored.

The description should be as comprehensive as necessary to assist the public in understanding fully the ways and means information flows as the program functions.

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.

Digital refers generally to data in electronic or other non-paper format, such as internet sites, platforms, software, applications, databases, devices, and other electronic information technologies that an agency may sponsor or use to promote digital collaboration, participation, and transparency.

Mobile denotes data access, processing, communications, and storage by users in a dynamically located, real-time fashion, typically through portable devices and remote platforms.

SE-1 Inventory of Personally Identifiable Information

3.1.3 How do you retrieve information?

Click here to enter text.

Describe how you retrieve information from where you store it. Describe whether you retrieve information by name of the individual or by some identifying number, symbol, or other identifying particular, provide a detailed

3.1.3 How do you retrieve information?

description of the identifiers or retrieval elements.

You might store paper forms in a filing cabinet and retrieve it by name of the person who submitted the form or by date of submission. You might search a database using the name of the country where USAID is supporting several projects. You might search for a document in MS Word or Google Docs by the name of the project on which you are working.

TR-2 System of Records Notices and Privacy Act Statements

3.2 INFORMATION COLLECTION, USE, MAINTENANCE, AND DISSEMINATION

3.2.1 What types of personally identifiable information (PII) do you collect, use, maintain, or disseminate?

(Please check all that apply. If you choose Other, *please list the additional types of PII.)*

☐ Name, Former Name, or Alias

☐ Mother’s Maiden Name

☐ Social Security Number or Truncated SSN

☐ Date of Birth

☐ Place of Birth

☐ Home Address

☐ Home Phone Number

☐ Personal Cell Phone Number

☐ Personal E-Mail Address

☐ Work Phone Number

☐ Work E-Mail Address

☐ Driver’s License Number

☐ Passport Number or Green Card Number

☐ Employee Number or Other Employee Identifier

☐ Tax Identification Number

☐ Credit Card Number or Other Financial Account Number

☐ Patient Identification Number

☐ Employment or Salary Record

☐ Medical Record

3.2.1 What types of personally identifiable information (PII) do you collect, use, maintain, or disseminate?

(Please check all that apply. If you choose Other*, please list the additional types of PII.)*

☐ Criminal Record

☐ Military Record

☐ Financial Record

☐ Education Record

☐ Biometric Record (signature, fingerprint, photograph, voice print, physical movement, DNA marker, retinal scan, etc.)

☐ Sex or Gender

☐ Age

☐ Other Physical Characteristic (eye color, hair color, height, tattoo)

☐ Sexual Orientation

☐ Marital status or Family Information

☐ Race or Ethnicity

☐ Religion

☐ Citizenship

☐ Other: Click here to enter text.

☐ None

Personally Identifiable Information (PII) means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

SE-1 Inventory of Personally Identifiable Information

3.2.2 About what types of people do you collect, use, maintain, or disseminate personal information?

(Please check all that apply. If you choose Other, *please provide the types of people.)*

☐ Citizens of the United States

☐ Aliens lawfully admitted to the United States for permanent residence

☐ USAID employees, including Foreign Service National (FSN) Direct Hires, FSN Personal Services Contractors, and Third Country National Employees

☐ Employees of USAID contractors or service providers

☐ Visitors to the United States

☐ Aliens

☐ Business Owners or Executives

☐ 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?

(Please check all that apply. If you choose Other, *please provide the types of data.)*

☐ Log Data (IP address, time, date, referrer site, browser type)

☐ Tracking Data (single- or multi-session cookies, beacons)

☐ Form Data

☐ User Names

☐ Passwords

☐ Unique Device Identifier

☐ Location or GPS Data

☐ Camera Controls (photo, video, videoconference)

☐ Microphone Controls

☐ Other Hardware or Software Controls

☐ Photo Data

☐ Audio or Sound Data

☐ Other Device Sensor Controls or Data

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?

(Please check all that apply. If you choose Other*, please provide the types of data.)*

☐ On/Off Status and Controls

☐ Cell Tower Records (logs, user location, time, date)

☐ Data Collected by Apps (itemize)

☐ Contact List and Directories

☐ Biometric Data or Related Data

☐ SD Card or Other Stored Data

☐ Network Status

☐ Network Communications Data

☐ Device Settings or Preferences (security, sharing, status)

☐ Other: Click here to enter text.

☐ 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 *could be* made available to USAID or its contractors and service providers?

Click here to enter text.

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.

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.

Make PII available 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.

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.

UL-1 Internal Use

3.2.8 With whom do you share the PII outside of USAID?

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).

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?

(Please check all that apply. If you choose New Technology *or* Other, *please explain.)*

☐ Network

☐ Database

☐ Software

☐ Hardware

☐ Mobile Application or Platform

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

3.3.3 What is the system status? *(If this is an existing Information Collection, please enter the OMB Control Number. If you choose* Other, *please explain.)*
☐ New System Development or Procurement
☐ Existing System Being Updated
☐ Existing Information Collection OMB Control Number: Click here to enter text.

3.3.3 What is the system status?

(If this is an existing Information Collection, please enter the OMB Control Number. If you choose Other, *please explain.)*

☐ New Data Collection Form or Survey

☐ Request for Dataset to be Published on an External Website

☐ 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?

(If you choose Yes, *please provide the specifics of any new privacy risks and mitigation strategies.)*

☐ No.

☐ 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?

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

☐ 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 Website or Application 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.

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

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.)

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

4. PRIVACY RISKS AND CONTROLS

The questions in this section focus on the specific privacy risks of your system and the mitigation strategies (controls) that help you reduce the risks of collecting, using, maintaining, and disseminating PII. The Privacy Controls focus on information privacy as a value distinct from, but interrelated with, information security. The Privacy Controls are the administrative, technical, and physical safeguards employed within USAID to protect and ensure the proper handling of PII. For more in-depth information about these Privacy Controls, please see Appendix D Privacy Controls.

4.1 AUTHORITY AND PURPOSE (AP)

The Authority and Purpose Privacy Control Family ensures that USAID identifies the legal bases that authorize a particular PII collection or activity; and specifies in its notices the purposes for which PII is collected.

4.1.1 Why is the PII collected and how do you use it?

Click here to enter text.

Describe purposes of the PII collection and connect the purposes to a USAID business function.

Describe specifically how you will use the PII to accomplish the purposes provided in the previous section. Describe why the PII is necessary to accomplish the purposes.

Example: The PII is collected on an application form and is used to determine eligibility for a new grant under the HIV/AIDs education program.

Example: USAID is collecting the PII through an on-line survey to determine the effectiveness of USAID programs. The result of the survey will be analyzed by gender, age group, and ethnicity to determine outreach areas for USAID's development programs.

AP-2 Purpose Specification

4.1.2 What are your processes and procedures for identifying and evaluating any proposed new uses of the PII?

Click here to enter text.

Are there any privacy risks for this system that relate to the purposes specified at the time of the collection? If so, how will you mitigate these risks? Discuss any privacy risks associated with the purpose of the information in the project. For example, are all the purposes for which the information may be used specified at the time of collection? If not, why not? If information may later be used for reasons other than the purposes specified, will individuals have the opportunity to consent to the new use? Discuss how any associated risks are mitigated. If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.

AP-2 Purpose Specification
AR-4 Privacy Monitoring and Auditing

4.2 ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (AR)

The Accountability, Audit, and Risk Management Privacy Control Family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that USAID is complying with applicable privacy protection requirements and minimizing overall privacy risk.

4.2.1 Do you use any data collection forms or surveys?

(If you choose Yes*, please provide the OMB Control Number and USAID control number.)*

☐ No.

☐ Yes: Click here to enter text.

Attach a copy of the form or the survey as an appendix to the PIA. If there are multiple forms or surveys, attach a copy of the forms or surveys in the appendix and include a list in the response to this question within the PIA. State whether these forms or surveys include a Privacy Act Notice or Statement that describes the authorities to collect PII, the PII purposes and uses, and the effects on the individual of not providing the PII.

Before you use any forms or surveys to collect personal information outside of your immediate office, you must contact and work with the Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD), pursuant to the USAID policies and procedures in ADS 505, Forms Management Program, and ADS 506, Reports Management. IRD will assist you to determine whether you will need to get USAID and/or OMB approval, and to complete the USAID and/or OMB approval processes, if needed.

AR-2 Privacy Impact and Risk Assessment

4.2.2 If the PII is being migrated from a legacy system to a new system, what safeguards are in place to mitigate the privacy risks of transferring the PII from the old to the new system?

Click here to enter text.

Describe the procedures you have created to manage the risk of transferring PII from one system to another and how you will monitor those procedure to ensure that they work appropriately.

AR-2 Privacy Impact and Risk Assessment
AR-4 Privacy Monitoring and Auditing

4.2.3 What privacy requirements have you included in contracts and other acquisition-related documents, pursuant to the Federal Acquisition Regulation (FAR) and compliance with the Privacy Act, FISMA, and other privacy requirements?

Click here to enter text.

Provide the contract numbers and verification that the contract contains the appropriate privacy clauses pursuant to the FAR (48 CFR): 1) Part 24, Protection of Privacy and Freedom of Information; and 2) Part 52, Solicitation Provisions and Contract Clauses (52.224-1, Privacy Act Notification, and 52.224-2, Privacy Act). Please explain

4.2.3 What privacy requirements have you included in contracts and other acquisition-related documents, pursuant to the Federal Acquisition Regulation (FAR) and compliance with the Privacy Act, FISMA, and other privacy requirements?

whether the privacy clauses cover third-party service providers and subcontractors to the contractors. You should include information on government contractors, cloud computing service provider contracts, and all other service-provider contracts and terms of service.

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing

4.2.4 What requirements have you included in contracts and other acquisition-related documents to ensure that 1) USAID owns and controls the PII in the system for the length of the contract and beyond, 2) the contractor or service provider has no ownership of the PII, and 3) the contractor or service provider has no access or retention rights to the PII beyond those authorized by the contract during the life of the contract?

Click here to enter text.

Describe how you ensure that government contractors and cloud computing service providers have no ownership rights over the PII and no access or retention rights after the close of a contract. Please explain whether the contract language covers third-party service providers and subcontractors to the contractors.

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing
UL-1 Internal Use

4.2.5 How do you audit and/or monitor system and user activity to ensure that the administrative, technical, and physical security safeguards you use actually do guard against privacy risks?

Click here to enter text.

Describe how you ensure that the PII is used in accordance with the stated practices in this PIA. Discuss auditing measures, as well as technical and policy safeguards such as information sharing protocols, special access restrictions, and other controls (for example, “read-only” access capability). Explain whether the system will conduct the audits or whether third parties, such as the Office of the Inspector General or the Government Accountability Office, will conduct reviews.

AR-4 Privacy Monitoring and Auditing

4.2.6 How do you ensure that USAID employees, contractors, and service providers understand their responsibility to protect PII and the procedures for protecting PII?

Click here to enter text.

Describe privacy training and awareness activities, and provide any privacy rules of behavior documents.

4.2.6 How do you ensure that USAID employees, contractors, and service providers understand their responsibility to protect PII and the procedures for protecting PII?

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing
AR-5 Privacy Awareness and Training
UL-1 Internal Use

4.2.7 If you collect PII under a pledge of confidentiality for exclusively statistical purposes, how do you ensure that the PII is not disclosed or used inappropriately?

Click here to enter text.

Attach a copy of the collection statement and any form or survey as an appendix to the PIA. If there are multiple forms or surveys, attach a copy of the forms or surveys in the appendix and include a list in the response to this question within the PIA.

Statistical purpose (A) means the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; and (B) includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support the purposes described in subparagraph (A).

Describe how you ensure that the PII is used for the specified statistical purposes only. Describe also how you ensure that the PII is not disclosed without the consent of the respondent. Describe how you ensure that, when the PII is disclosed without the respondent's consent, the disclosure is authorized by the USAID Administrator.

Respondent means a person who, or organization that, is requested or required to supply information to an agency, is the subject of information requested or required to be supplied to an agency, or provides that information to an agency.

AR-2 Privacy Impact and Risk Assessment
AR-4 Privacy Monitoring and Auditing
UL-1 Internal Use
UL-2 Information Sharing with Third Parties

4.2.8 What other risks to privacy exist and how do you manage these risks?

Click here to enter text.

Explain how you identify and manage any additional privacy risks. Describe any privacy risks and controls that relate to the systems technology you use, rather than the PII involved.

AR-2 Privacy Impact and Risk Management

4.3 DATA QUALITY AND INTEGRITY (DI)

The Data Quality and Integrity Privacy Control Family enhances public confidence that any PII collected and maintained by USAID is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

4.3.1 How do you ensure that you collect information to the greatest extent possible directly from the subject individual?

Click here to enter text.

Discuss whether the PII is collected directly from the individual or collected from another source. If the PII is not being collected from the individual, but from sources other than the individual, you must explain why collecting the PII from other sources is required. Sources other than the individual may include other individuals, systems, systems of records, businesses, commercial data aggregators, other Federal agencies, and state or local agencies.

Describe your sources of information when you use digital collaboration tools or services and/or mobile services.

Digital refers generally to data in electronic or other non-paper format, such as internet sites, platforms, software, applications, databases, devices, and other electronic information technologies that an agency may sponsor or use to promote digital collaboration, participation, and transparency.

Mobile denotes data access, processing, communications, and storage by users in a dynamically located, real-time fashion, typically through portable devices and remote platforms.

DI-1 Data Quality

4.3.2 How do you ensure, to the greatest extent possible, that the PII is accurate, relevant, timely, and complete at the time of collection?

Click here to enter text.

Describe how what reasonable steps you take to confirm the accuracy and relevance of PII. Such steps may include editing and validating addresses as they are collected or entered into the system using automated address verification look-up application programming interfaces. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

DI-1 Data Quality

4.3.3 How do you check for, and correct as necessary, any inaccurate or outdated PII in the system?

Click here to enter text.

Describe how you will ensure that the PII continues to remain accurate, relevant, timely and complete over time. Describe what reasonable steps you take to confirm the accuracy and relevance of PII after the initial collection of the PII. Such steps may include periodic quality control auditing.

DI-1 Data Quality

4.4 DATA MINIMIZATION AND RETENTION (DM)

The Data Minimization and Retention Privacy Control Family helps USAID to implement the data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. USAID retains PII for only as long as necessary to fulfill the purposes specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

4.4.1 What are the minimum PII elements that are relevant and necessary to accomplish the legal purpose of the program?

(If you choose Yes*, please explain the business need for the PII elements.)*

Click here to enter text.

Describe why you need the specific PII elements that you collect in order to fulfill the business functions of the program. If you use SSNs, please explain why you need SSNs to fulfill a business function and why your program could not operate without them.

Describe any impacts on business functions from not being able to collect, use, maintain, or disseminate the specific PII elements. Describe any decision made to collect less data than originally planned. Align your explanation with the Purpose section of any relevant System of Records Notice (SORN). A general statement about the purpose without discussing particular PII is not an adequate response.

DM-1 Minimization of Personally Identifiable Information

4.4.2 How do you monitor the PII and the system to ensure that only the PII identified in the privacy notices is collected, used, maintained, and disseminated by the system and that the PII continues to be necessary to accomplish the legally authorized purpose?

Click here to enter text.

Describe how you ensure that you do not collect more PII than stated in the privacy notice. Describe how you ensure that all of the PII elements collected continue to be necessary for the stated purpose.

AR-4 Privacy Monitoring and Auditing
DM-1 Minimization of Personally Identifiable Information

4.4.3 Does the system derive new data or create previously unavailable data about an individual through aggregation or derivation of the information collected? Is the PII relevant and necessary to the specified purposes and how is it maintained?

(If you choose Yes*, please explain.)*

☐ No.

☐ Yes: Click here to enter text.

Discuss whether the system will aggregate or derive data. State whether a unique identifier may be generated by the system and provided to the user for future follow up. Describe how the new PII will be used and why it is relevant and necessary to the system.

Modernized systems often have the capability to derive new data and create previously unavailable data about an individual through aggregation of the information collected. The *mosaic effect* is the idea that disparate pieces of

4.4.3 Does the system derive new data or create previously unavailable data about an individual through aggregation or derivation of the information collected? Is the PII relevant and necessary to the specified purposes and how is it maintained?

(If you choose Yes*, please explain.)*

information, though individually of limited or no value, can be significant when combined with other pieces of information that could result in an unforeseen vulnerability, exploitation or misuse of the information.

Derived data is information obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information.

Data aggregation is the taking of various data elements and then turning them into a composite of all the data to form another type of data (i.e., tables or data arrays) that is usually different from the source information.

DM-1 Minimization of Personally Identifiable Information

4.4.4 What types of reports about individuals to do produce from the system?

Click here to enter text.

Describe each report that will be produced and what PII will be included. Discuss the use for the reports, and who will have access to the reports inside and with whom you will share the reports outside USAID.

In addition, discuss whether the report will produce anonymized data. If data will not be anonymized, discuss why. Explain the risks that the PII can be combined with other data either to identify an individual or used in ways that the individual did not intend.

Anonymized data means data from which the individual cannot be identified by the recipient of the information. Sometimes known as de-identified. To anonymize or de-identify PII in a report, individuals' names, addresses, and full postal/zip codes must be removed together with any other information which, in conjunction with other data held by or disclosed to the recipient, could identify the individual.

DM-1 Minimization of Personally Identifiable Information

4.4.5 How do you file, maintain, and store the PII? How long do you retain the PII? What methods do you use to archive and/or dispose of the PII? How do you ensure that the records management retention rules specified above are followed?

Click here to enter text.

The program manager, in consultation with a records management officer, must develop a records retention schedule for the records contained in the system. After the records schedule is developed, it is sent to the National Archives and Records Administration (NARA) for approval. Consult with your records management office for assistance with this question, if appropriate.

If a NARA-approved records schedule exists, please provide the records schedule and explain for how long and for what reason the PII is retained. If a general records schedule (GRS) covers the information, then please provide the GRS number (GRS X, Item X) and explain for how long and for what reason the PII is retained.

If there is not an approved NARA records schedule or GRS, then the project manager should consult with the records management officer to develop a records retention schedule for the records contained in the system for the minimum amount of time necessary to fulfill the needs of the project. If a NARA-approved schedule does not exist, explain what stage the project is in developing and submitting a records retention schedule.

Describe the processes used to dispose of the PII when it is no longer needed.

Describe how you ensure that the PII is retained only as long as it is needed and that the PII is destroyed in an appropriate manner.

AR-4 Privacy Monitoring and Auditing
DM-2 Data Retention and Disposal

4.4.6 Does the system monitor or track individuals?

(If you choose Yes, *please explain the monitoring capability.)*

☐ No.

☐ Yes: Click here to enter text.

Describe how you monitor individuals, and explain the purpose of the monitoring. Discuss whether someone reviews any logs created by the monitoring. Discuss the safeguards you have created to prevent abuse. Include how the decision was made to move forward with a monitoring capability and what safeguards are in place to reduce impact on personal privacy. If the system has the capability to monitor individuals, but that capability is not be used, describe how you will ensure that such monitoring capability will not be used.

Describe how you track individuals by using tracking technologies that will compile or make such data available to USAID. Describe how other persons or agencies (app developer, original equipment manufacturer, network or carrier, cloud service provider) will use tracking technology. Describe how the system could enable other persons or agencies to determine the location of individuals and whether such location data could compromise the physical safety of the individuals or the security of USAID operations.

IP-1 Consent
TR-1 Privacy Notice

4.4.7 What policies, procedures, and control methods do you follow to minimize the use of PII for and protect PII during testing, training, and research?

Click here to enter text.

Discuss whether you use PII for testing update or new applications prior to deployment and whether you also use PII for research purposes and for training. The use of PII in testing, research, and training increases the risk of unauthorized disclosure or misuse of the PII. Describe the measures you take to minimize any associated privacy risks. Also provide the authorities that allow you to use PII for testing, training, and research.

AP-2 Purpose Specification
AR-4 Privacy Monitoring and Auditing
DM-3 Minimization of PII Used in Testing, Training, and Research

4.5 INDIVIDUAL PARTICIPATION AND REDRESS (IP)

The Individual Participation and Redress Privacy Control Family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in USAID decisions made based on the PII.

4.5.1 What opportunities for consent do you provide to individuals regarding what PII is collected and how that PII is shared?

Click here to enter text.

Discuss whether the PII collection is mandatory or voluntary and how the information is collected, such as via an application form, survey, web form, or extracted from other systems. Discuss whether an individual has the opportunity to consent to specific uses or whether consent is given to cover all current uses of the PII. Describe the process by which consent is given. If the individual can decline or opt out, describe how this is done. Describe the process by which consent is obtained for new uses of the PII after the initial collection. If no opportunities are available to individuals to consent, decline, or opt out, please explain why not.

IP-1 Consent
TR-1 Transparency

4.5.2 What mechanism do you provide for an individual to gain access to and/or to amend the PII pertaining to that individual?

Click here to enter text.

Describe any procedures you provide for individuals to access their PII and to request correction or amendment of their PII, in addition to the USAID Freedom of Information Act (FOIA) and/or Privacy Act procedures under 22 CFR Part 215.

If you provide such additional access and amendment procedures, describe how you, consistent with the Privacy Act, keep (for the life of the record or five years after disclosure) an accurate accounting of disclosures of PII including 1) date, nature, and purpose of each disclosure; and 2) name an address of the person or federal agency to

4.5.2 What mechanism do you provide for an individual to gain access to and/or to amend the PII pertaining to that individual?

which the disclosure was made.

If individuals cannot access or amend or correct their PII under the USAID FOIA/Privacy Act procedures, explain why not.

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.

AR-8 Accounting of Disclosures
IP-2 Individual Access
IP-3 Redress

4.5.3 If your system involves cloud computing services and the PII is located outside of USAID, how do you ensure that the PII will be available to individuals who request access and redress?

Click here to enter text.

Describe how you ensure that the program manager is able to produce the records when an individual requests access to and amendment of his/her personal information through the USAID Freedom of Information Act or Privacy Act request process. Please explain whether your protections cover records or systems controlled by third-party service providers and/or subcontractors to contractors.

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing
IP-2 Individual Access
IP-3 Redress

4.6 SECURITY (SE)

The Security Privacy Control Family 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.

4.6.1 How do you secure the PII? What administrative, technical, and physical security safeguards do you use to guard against privacy risks such as 1) data loss or breach; 2) unauthorized access, use, destruction, or modification; 3) unintended or inappropriate disclosure; or 4) receipt by an unauthorized recipient?

Click here to enter text.

Provide an overview of the mitigation strategies you use to protect the PII collected, used, maintained, and disseminated by your system.

4.6.1	**How do you secure the PII? What administrative, technical, and physical security safeguards do you use to guard against privacy risks such as 1) data loss or breach; 2) unauthorized access, use, destruction, or modification; 3) unintended or inappropriate disclosure; or 4) receipt by an unauthorized recipient?**
Describe the steps taken to ensure that the PII is used appropriately. Indicate any physical controls that will be implemented (security guards, identification badges, key cards, safes, locks, etc.). Indicate any technical controls that will be implemented (user identification, password, intrusion detection, encryption firewall, etc.). List any administrative controls that will be implemented (periodic security audits, regular monitoring of users, backup of sensitive data, etc.). Describe any mechanisms in place to identify security breaches. Discuss what privacy incident reporting plan and procedures are in place to effectively handle a privacy incident involving the system. Describe the extra mitigation strategies do you use to guard against the heightened privacy risks associated with any collection, use, maintenance, or dissemination of Names with SSNs. *Example:* Describe the steps you take to make sure that transmitted data is properly secured through encryption or by classified couriers. *Example:* Describe the steps you take to develop or modify processes and procedures to account for identified privacy risks related to the increased frequency of access to audit logs.	
SE-1 Inventory of Personally Identifiable Information SE-2 Privacy Incident Response	

4.6.2	**If your system is controlled by a contractor or service provider, what requirements have you included in contracts and other acquisition-related documents to detail the procedures for privacy breach liability and response?**
Click here to enter text.	
Describe how you ensure that government contractors and cloud computing service providers have privacy incident response procedures and that they follow those procedures. Explain whether the contract language allocates any responsibility and liability for privacy breach response.	
AR-3 Privacy Requirements for Contractors and Service Providers AR-4 Privacy Monitoring and Auditing SE-2 Privacy Incident Response	

4.7 TRANSPARENCY (TR)

The Transparency Privacy Control Family ensures that USAID provides public notice of its information practices and the privacy impact of its programs and activities.

4.7.1	**How do you provide notice to individuals regarding 1) the authority to collect PII; 2) the principal purposes for which the PII will be used; 3) the routine uses of the PII; and 4) the effects on the individual, if any, of not providing all or any part of the PII?**
Click here to enter text.	
Provide a copy of any written notice that you provide before you collect, use, maintain, or disseminate PII, including	

4.7.1 How do you provide notice to individuals regarding 1) the authority to collect PII; 2) the principal purposes for which the PII will be used; 3) the routine uses of the PII; and 4) the effects on the individual, if any, of not providing all or any part of the PII?

any: 1) posted privacy policy; 2) Privacy Act Statement, pursuant to the Privacy Act (e)(3); on forms or surveys; 3) System of Records Notice; or 4) other information provided on the USAID website. Provide a copy of any notice you provide directly to the individuals whose PII you collect.

If you collect the PII from someone other than the individual, explain how that PII is collected and how the individual is provided notice.

If notice was not provided, explain why not.

Describe how you monitor or audit privacy notices to ensure that on a continuing basis the notice statements are accurate and appropriately placed.

AR-4 Privacy Monitoring and Auditing
TR-1 Privacy Notice
TR-2 System of Records Notices and Privacy Act Statements

4.7.2 Have you or will you publish a Privacy Act System of Records Notice (SORN) for this system?

(If you choose Yes*, please provide information about the SORN, including the name, date, and Federal Register citation.)*

☐ No

☐ Yes: Click here to enter text. and Click here to enter a date.

For all systems of records, the Privacy Act requires that the agency publish a SORN in the Federal Register. Include the Federal Register citation for the SORN. If the information used in the project did not require a SORN, explain why not. In some instances, an existing SORN (either program-specific, USAID-wide, or Government-wide) may apply to the system's collection of information. In other instances, a new SORN may be required.

USAID SORNs are available at **http://www.usaid.gov/privacy-policy/systems-records-notices-sorns.** That web page also has links to government-wide SORNs and Office of Personnel Management SORNs, which might be applicable to your system of records.

TR-2 System of Records Notices and Privacy Act Statements

4.7.3 If your system involves cloud computing services and the PII is located outside of USAID, how do you ensure that you know the location of the PII and that the SORN System Location(s) section provides appropriate notice of the PII location?

Click here to enter text.

Describe how you ensure that any cloud computing services providers do not move the PII or move it without notice to you.

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing
TR-2 System of Records Notices and Privacy Act Statements

4.8 USE LIMITATION (UL)

The Use Limitation Privacy Control Family 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.

4.8.1 How do you monitor access to and use of the system to ensure that the PII is collected, accessed, and used only 1) for the authorized purposes and 2) by authorized USAID employees, contractors, and service providers?

Click here to enter text.

Describe how you ensure that the system uses PII only in ways that are compatible with the specified purposes.

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.

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing
UL-1 Internal Use

4.8.2 If you share PII outside of USAID, how do you ensure the protection of the PII 1) as it moves from USAID to the outside entity and 2) when it is used, maintained, or disseminated by the outside entity?

(If you choose Yes, please provide the specifics of the agreement or a copy of the agreement.)

Click here to enter text.

State whether there is a MOU, contract, or agreement in place and define the parameters of the sharing agreement. Describe any agreement that covers the terms of the information sharing, including 1) a specific description of the PII covered, 2) an enumeration of the purposes for which the PII may be used, 3) monitoring, auditing, and training requirements, and 4) the consequences for unauthorized access to and use of the PII.

Describe what privacy controls you use to reduce the risk of transmitting data to systems outside of USAID. Describe how the data is transmitted outside of USAID. For example, describe whether the data transmitted electronically, in bulk, by paper, direct access, or by some other means. Discuss whether access controls have been implemented to ensure appropriate sharing of information.

Discuss whether the receiving system has undergone a Certification & Accreditation (C&A). For sharing with non-Federal agencies, discuss how the relevant privacy protections have been expressed and documented to ensure the privacy and security of the information once it is shared. If necessary, discuss the provisions for notification of a privacy incident and who owns the liability for such incident.

When using digital collaboration services and/or mobile services, describe how you will share data outside of USAID. Specifically, describe how you will expose or transmit the data to a third-party or how the third-party will access the data.

Digital refers generally to data in electronic or other non-paper format, such as internet sites, platforms, software, applications, databases, devices, and other electronic information technologies that an agency may sponsor or use to promote digital collaboration, participation, and transparency.

Mobile denotes data access, processing, communications, and storage by users in a dynamically located, real-time fashion, typically through portable devices and remote platforms.

AR-4 Privacy Monitoring and Auditing
UL-2 Information Sharing with Third Parties

4.9 THIRD-PARTY WEBSITES AND APPLICATIONS

The OMB policy in *Guidance for Agency Use of Third-Party Websites and* Applications, M-10-23 (June 25, 2010), requires USAID to take specific steps to protect individual privacy whenever it uses third-party websites and applications to engage with the public. Through the following questions, USAID ensures individual notice and careful analysis of the privacy implications when using third-party websites and/or applications. Please answer the following questions, if your system involves a third-party website or application.

The term "*third-party websites or applications*" refers to 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.

4.9.1 What PII might become available to you when the third-party website or application makes information available to you through public use?

Click here to enter text.

Describe the types of PII that might become available to you through public use of the third-party website or application. Please refer to the list of PII examples in PIA Section 3.2.1 *What types of PII do you collect, use, maintain, or disseminate?*

Describe how you will handle any PII that becomes available to you beyond what you are authorized and have a business need to collect, use, maintain, or disseminate.

Make PII available 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.

AP-1 Authority to Collect

4.9.2 How do you ensure that the privacy policy of the third-party website and/or application is reviewed to ensure that it appropriately supports the USAID privacy protection position?

Click here to enter text.

Explain how you ensure, in consultation with legal counsel and relevant program managers, that the content of the third-party public notices comply with USAID privacy requirements. Please provide a link to the privacy policy.

AR-3 Privacy Requirements for Contractors and Service Providers
TR-1 Privacy Notice

4.9.3 If you have a link from USAID.gov to this third-party website or other location that is not a part of an official government domain, do you provide an alert (such as a statement or "pop-up") to visitors explaining that they are being directed to a non-governmental website that may not afford the same privacy protections as USAID?

Click here to enter text.

Describe how you explain to the public that the website or application is not a government website or application, that it is controlled or operated by a third party, and that the USAID Website Privacy Policy does not apply to this third-party website or application.

AR-3 Privacy Requirements for Contractors and Service Providers
TR-1 Privacy Notice

4.9.4 If you incorporate or embed the third-party application on the USAID website, how do you disclose to the public the third-party application?

(If you choose Yes*, please describe the disclosure.)*

Click here to enter text.

A copy of the USAID Website Privacy Notice is provided at **http://www.usaid.gov/privacy.html**. If the collection and/or storage of PII through your third-party application is different from the process described in the USAID Website Privacy Notice, please describe the third-party application involvement.

For example, the third-party website can provide individuals with itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, the third-party website must include consent mechanisms to ensure that the website operations comply with individual choices.

TR-1 Privacy Notice

4.9.5 How do you create the appropriate USAID brand to indicate an official USAID presence on the third-party website, and how you distinguish USAID activities from those of non-governmental actors?

Click here to enter text.

Describe how you apply appropriate branding to distinguish USAID activities from those of non-governmental actors, when you use a third-party website or application that is not part of an official government domain. For example, do you, to the extent practicable, add the USAID seal or emblem to the USAID profile page on a social media website to indicate that it is an official agency presence? Please list activities that a government individual can perform on this third-party website or application that the public is not allowed to see.

TR-1 Privacy Notice

STOP 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.

- 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 PIA is ready for the approval process, the Privacy Office will send you this form to sign.

5. APPENDICES

5.1 APPENDIX A GLOSSARY

The following table describes terms and abbreviations used in this document.

Table 5-1 Glossary

Abbreviations	Description
ADS	USAID Automated Directives System
Alien	Someone who is not citizen of the United States or an alien lawfully admitted for permanent residence.
Anonymized Data	Data from which the individual cannot be identified by the recipient of the information. The name, address, and full post code must be removed together with any other information which, in conjunction with other data held by or disclosed to the recipient, could identify the individual.
Automated Directives System	
C&A	Certification & Accreditation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
Cloud Computing	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). (NIST SP 800-145)
CISO	Chief Information Security Officer
D	Draft Version
Data Aggregation	The taking of various data elements and then turning them into a composite of all the data to form another type of data (i.e., tables or data arrays) that is usually different from the source information
Derived Data	Information obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information
Digital	Refers generally to data in electronic or other non-paper format, such as internet sites, platforms, software, applications, databases, devices, and other electronic information technologies that an agency may sponsor or use to promote digital collaboration, participation, and transparency
F	Final Version
FIPS PUB	NIST Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
Foreign Service National Direct Hire (FSNDH) Employee	Means 1) a non-U.S. citizen employee hired by a USAID Mission abroad, whether full or part-time, intermittent or temporary, and inclusive of a Third Country National (TCN) who is paid under the local compensation plan (LCP), and 2) who was appointed under the authority of the Foreign Service Act of 1980.
Foreign Service National Personal Services Contractor (FSNPSC) Employee	Means 1) a non-U.S. citizen employee hired by a USAID Mission abroad, whether full or part-time, intermittent, or temporary, and inclusive of a Third Country National (TCN) who is paid under the local compensation plan (LCP), and 2) who entered in a contract pursuant to the AIDAR, Appendix J.
IA	Information Assurance, Office of the Chief Information Security Officer

Abbreviations	Description
IIF	Information in Identifiable Form
Individual	A citizen of the United States or an alien lawfully admitted for permanent residence. (5 USC 552a)
Information in Identifiable Form (IIF) *See Personally Identifiable Information*	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means (for example, name, SSN, date of birth, or medical history (44 USC 3501, note § 208); or information permitting the physical or online contacting of a specific individual. (M-03-22)
Information System Security Officer (ISSO)	Individual responsible to the senior agency information security officer, AO, or information SO for ensuring the appropriate operational security posture is maintained for an information system or program. (Chapters 508 and 545)
Information Technology	Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use— (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related re- sources; but does not include any equipment acquired by a federal contractor incidental to a federal contract (40 USC 11101); or 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. (M-03-22)
M	Memorandum or Bureau of Management
Make PII Available	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.
Mobile	Denotes data access, processing, communications, and storage by users in a dynamically located, real-time fashion, typically through portable devices and remote platforms
Mosaic Effect	When disparate pieces of information, though individually of limited or no value, can be significant when combined with other pieces of information that could result in an unforeseen vulnerability, exploitation or misuse of the information
MOU	Memoranda of Understanding
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
Person	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. (44 USC 3502)
Personally Identifiable Information (PII)	Information that directly identifies an individual. PII examples include name, address, social security number, or other identifying number or code, telephone

Abbreviations	Description
	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". (ADS 508)
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PO	Privacy Office
POA&M	Plan of Action and Milestones
Privacy Impact Assessment	An 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, [using,] maintaining and disseminating information in identifiable form in an electronic information system, and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. (M-03-22)
Program Manager (PM)	Government official responsible and accountable for the conduct of a government program. A government program may be large (e.g., may provide U.S. assistance to other nations); it may also be a support activity such as the Agency's personnel or payroll program. (Chapters 508, 545, 552, 629)
SORN	System of Records Notice
SP	NIST Special Publication
SSN	Social Security Number
System	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. (ADS 508)
System Owner (SO)	Individual responsible for daily program and operational management of their specific USAID system. System Owners are responsible for ensuring that a security plan is prepared, implementing the plan and monitoring its effectiveness. (Chapters 508 and 545)
Third Country National (TCN) Employee	An individual who is 1) neither a U.S. citizen nor a permanent legal resident alien of the United States nor a host-country citizen, and 2) eligible for return travel to the home country or country of recruitment at U.S. Government expense.
Third-Party Websites or Applications	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.
USAID	United State Agency for International Development
USC	United States Code

5.2 APPENDIX B CONDUCTING THE PIA

5.2.1 Background

The E-Government Act mandates that all federal agencies conduct a Privacy Impact Assessment (PIA) when they use information technology (systems) to collect, use, maintain, or disseminate personally identifiable information (PII). PIAs provide information on how agencies handle PII, so that the American public has assurances that their PII is protected by their government.

The PIA is a risk-based analysis that enables USAID to determine the level of risk acceptable to the systems that support the conduct of USAID business functions. Risk mitigation helps USAID to 1) cost-effectively reduce information privacy risks to an acceptable level, 2) address information privacy throughout the life cycle of each system, and 3) ensure compliance with the federal authorities and USAID policies, procedures, and standards. The PIA's risk mitigation function works hand-in-hand with USAID's Certification and Accreditation (C&A), Security Controls Assessments (SCA), Risk Assessment, and Plan of Action and Milestones (POA&M) processes.

The PIA process should accomplish two goals: 1) determine the risks and effects of collecting, using, maintaining, and disseminating PII; and 2) evaluate protections and alternative processes for handling PII to mitigate potential privacy risks. The length and breadth of a PIA will vary by the size and complexity of the program or system. Any new system that involves the processing of PII should be able to demonstrate, through the PIA, that an in-depth analysis was conducted to ensure that privacy protections were built into the system.

This PIA Template is being used to gather information from program managers, system owners, and information system security officers. The information provided will be used by the Privacy Officer to analyze the privacy risks and controls for each system.

If you have questions about or would like assistance with this PIA Template, the PIA process, or other privacy compliance requirements please contact the USAID Privacy Office at **privacy@usaid.gov**.

5.2.2 Using this Word Template

This PIA form is a fillable Word template, which means that you can fill in the information in the appropriate fields, save the document, and submit the PIA electronically as an e-mail attachment. To create a PIA Word document from this PIA Template, use the following steps:

1. Click on **File** and then **Save As**.
2. In the **Save As** window save your PIA using the name provided; just update the date and version number with D for draft.
3. Then select **Word Document (*.docx)** from the **Save as type**: drop-down list.

5.2.3 Completing the PIA Template

This PIA Template has various fields to be completed. First, fill in or update the fields on the Title Page, Headers and Footers, and Change History Page.

- Fill in or edit, if appropriate, the Program Name and System Name sections on the title page. Update the Version number on the title page. The Approved date on the title page will be completed at the end of the process.
- Fill in the System Name field in the Header, and the Date field in the Footer. The date in the Footer should be the date you send this PIA to the Privacy Office for review.
- Update the Change History page to reflect your new version of this PIA. The date in the Change History should be the date you send this PIA to the Privacy Office for review.

Complete the contact information in Section 2: Contact Information and Approval Signatures. Insert the appropriate Name, Title, Office Name, Office Phone Number, and E-Mail address for the Program Manager, System Owner, and Information System Security Officer.

Continue to Section 3: Information, and answer the questions.

5.2.4 Answering the Questions

PIAs are formal documents and can be made available to the public on the USAID website and upon request. Therefore, when completing this template, please respond to each question as if speaking to a member of the general public who is learning of this system for the first time.

- Each question has an answer box. Some answer boxes are simple text boxes, while other answer boxes have items to select, as appropriate.
- When you see a box (☐), you will be able to click on it to create a check mark to choose that item. Please select all items that apply. You should be able to add explanatory remarks in the answer boxes.
- Each section includes assistance (in blue text) on how to answer the question.
- Answer each question fully and completely. Answer each question with sufficient detail to permit the Privacy Office to analyze the privacy risks, controls, and risk mitigation plans.
- Type *Not Applicable* in the answer boxes for those questions that do not apply to your system and explain why the question is not applicable.
- Spell out each acronym the first time it is used in the PIA.
- Define technical terms or references, and keep in mind readers may not understand technical terms until they are explained.

- Use short and simple sentences.
- Use Spell Check and Grammar Check before submitting the PIA for approval.

5.2.5 Help Interpreting the Questions

Some questions provide choices, with the option to either pick one or pick all that apply. The questions that do not provide choices include explanations of the type of information that is required. At the end of each question, is a reference to the Privacy Controls, which provide more information on the topic. For more information on the Privacy Controls, please see **Appendix C Privacy Controls**.

5.3 APPENDIX C PRIVACY CONTROLS

Appendix J: Privacy Control Catalog in NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013). To access *Appendix J*, use this link (**Appendix J**).

Table 5-3 Privacy Controls

ID	Privacy Controls
AP Authority and Purpose	Ensures that USAID identifies the legal bases that authorize a particular PII collection or activity; and specifies in its notices the purposes for which PII is collected.
AP-1	Authority to Collect
AP-2	Purpose Specification
AR Accountability, Audit, and Risk Management	Enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that USAID is complying with applicable privacy protection requirements and minimizing overall privacy risk.
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI Data Quality and Integrity	Enhances public confidence that any PII collected and maintained by USAID is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.
DI-1	Data Quality
DI-2	Data Integrity and Date Integrity Board
DM Data Minimization and Retention	Helps USAID to implement the data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. USAID retains PII for only as long as necessary to fulfill the purposes specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP Individual Participation and Redress	Addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in USAID decisions made based on the PII.
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management

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