

SENSITIVE BUT UNCLASSIFIED



Management Bureau/Chief Information Officer/Information Assurance/
Privacy Office (M/CIO/IA/PO)

PRIVACY THRESHOLD ANALYSIS (PTA)

Global Research and Innovation Fellowship Network (GRIFN)

Version 1F

Approved: March 18, 2014

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

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.	May 31, 2013	1D	PTA Template.
2.	March 18, 2014	1F	Final
3.	Click here to enter a date.		36T
	36T		36T
	36T		36T

TABLE OF CONTENTS

1. INTRODUCTION.....	1
2. CONTACT INFORMATION AND APPROVAL SIGNATURES.....	2
3. PTA ANALYSIS	3
3.1 PROGRAM INFORMATION.....	3
3.2 INFORMATION COLLECTION.....	4
3.3 SYSTEM INFORMATION	8
4. APPENDICES.....	13
4.1 APPENDIX A GLOSSARY	13
4.2 APPENDIX B CONDUCTING THE PTA	15
4.3 APPENDIX C PRIVACY CONTROLS	17

1. INTRODUCTION

The USAID Privacy Office is using this Privacy Threshold Analysis (PTA) Template to gather information from program managers and system owners in order to discover any information privacy issues.

The PTA process should accomplish two goals: 1) determine whether a particular program will encounter any information privacy risks as it performs its functions; and 2) identify whether the program needs to comply with any privacy protection requirements pursuant to federal privacy statutes, regulations, and other authorities.

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. For more in-depth instructions on PTAs and how to complete this PTA Template, please see Appendix C Conducting the PTA.

If you have questions about or would like assistance with this PTA Template, the PTA 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: Courtney Matson
Title: Fellowship Program Manager
Office Name: OST
Office Phone #: 202-712-5604
E-Mail: cmatson@usaid.gov

SYSTEM OWNER

Name: Courtney Matson
Title: Fellowship Program Manager
Office Name: Global Development Lab
Office Phone #: 202-712-5604
E-Mail: cmatson@usaid.gov

Signature Date: March 19, 2014

Signature: C G Matson

PRIVACY ANALYST

Name: William Hoffman
Title: Privacy Office
Office Phone #: 703-666-1292
E-Mail: whoffman@usaid.gov

Signature Date: March 18, 2014

Signature: W C Hoffman

3. PTA ANALYSIS

3.1 PROGRAM INFORMATION

3.1.1 Describe the program and its purpose.
<p>USAID's Research and Innovation Fellowships program offers a unique opportunity to bring together the brightest minds in the critical fields of science, technology, and innovation (STI) to address complex development challenges. Through a partnership with the U.S. National Science Foundation (NSF) and drawing upon the resources of USAID's existing network of programs, the RI Fellowships will place promising talent from institutions around the United States with hosts in developing countries to help tackle the biggest development issues and engage in cutting-edge research and innovation. By building opportunities with in-country hosts through universities, non-governmental organizations, research institutions, government agencies, and private sector corporations, the RI Fellowships will help create relationships between new international partners, catalyze learning, and foster the positive exchange of information and experiences.</p>
<p>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.</p> <p>Describe the types of information that you use, and explain why and how you use the information.</p> <p>The description should be as comprehensive as necessary to assist the public in understanding the program fully.</p>
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?
<p>We plan to use a 3rd party website (screendoor.io) to host an online catalog of fellowship opportunities, where we will collect information about hosting opportunities and interested students. This same website will be used for students to access information about potential hosting opportunities and connect with those hosts directly. The information will be maintained on the same site.</p>
<p>Provide a general description of the paper documents, information systems, and/or electronic media that the program uses to meet 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.</p> <p>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.</p> <p>For this purpose, <i>system</i> 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.</p>

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?

Only an administrator (one of the three USAID team members) can go into the screendoor.io site and export the data collected as an excel file. That information will then be used to help us determine how many Fellows have been matched. Any data collected will be securely stored on USAID computers via the internal shared drive (accessible only to USAID team members)

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 description of the identifiers or retrieval elements.

You may 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 may search a database using the name of the country where a project in progress. You may 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

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

<input type="checkbox"/> Driver's License Number
<input type="checkbox"/> Passport Number or Green Card Number
<input type="checkbox"/> Employee Number or Other Employee Identifier
<input type="checkbox"/> Tax Identification Number
<input type="checkbox"/> Credit Card Number or Other Financial Account Number
<input type="checkbox"/> Patient Identification Number
<input checked="" type="checkbox"/> Employment or Salary Record
<input type="checkbox"/> Medical Record
<input type="checkbox"/> Criminal Record
<input type="checkbox"/> Military Record
<input type="checkbox"/> Financial Record
<input checked="" type="checkbox"/> Education Record
<input type="checkbox"/> Biometric Record (signature, fingerprint, photograph, voice print, physical movement, DNA marker, retinal scan, etc.)
<input checked="" type="checkbox"/> Sex or Gender
<input type="checkbox"/> Age
<input type="checkbox"/> Other Physical Characteristic (eye color, hair color, height, tattoo)
<input type="checkbox"/> Sexual Orientation
<input type="checkbox"/> Marital status or Family Information
<input checked="" type="checkbox"/> Race or Ethnicity
<input type="checkbox"/> Religion
<input checked="" type="checkbox"/> Citizenship
<input checked="" type="checkbox"/> Other: professional information about the supervisor (their expertise), information about the professional work environment, information about the desired timeline, information about the proposed development objectives, and information about what the host can provide the student in in-kind contributions.
<input type="checkbox"/> None
<p><i>Personally Identifiable Information (PII)</i> 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.</p> <p>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</p>

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 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.)

<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 checked="" type="checkbox"/> Form Data
<input checked="" type="checkbox"/> User Names
<input checked="" type="checkbox"/> Passwords
<input type="checkbox"/> Unique Device Identifier
<input checked="" 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
<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: 36T
<input type="checkbox"/> None
AR-2 Privacy Impact and Risk Assessment SE-1 Inventory of Personally Identifiable Information

3.2.3 What PII or digital or mobile data *could be* made available to USAID or its contractors and service providers?

The data mention in section 3.2.1 will only be available to the USAID team (3 members). The third party website (screendoor.io) used is open source software, and as such, we do not have a contractor or service provider, rather all data is managed by USAID. This being said, the technical host, Screendoor.io could have this data available to them for USAID’s purposes; they are on a contract/purchase order with USAID. The USAID administrators all have their own personal-generated passwords that allow them to access this information.

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

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

The USAID RI Fellowships program is being carried out under the authority of the foreign assistance act of 1961. All information is being provided voluntarily by the host institutions and Fellows in order to engage in this program.

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

3.2.5 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: The USAID RI Fellowships team owns and controls the information

☐ Another Federal Agency: 36T

☐ Contractor: 36T

☐ Cloud Computing Services Provider: 36T

☒ Third-Party Web Services Provider: Screendoor.io

☐ Mobile Services Provider: 36T

☒ Digital Collaboration Tools or Services Provider: Social networking/research sharing platform, as yet to be built

☐ Other: 36T

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

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

Our partners at NSF will have access to the Fellows' information. Currently the Fellows are already NSF grant recipients, so they are already in the NSF's system. In future iterations, Fellows' information will not be shared or made available beyond the Fellows' respective organization/academic institution/grantor stream that they are currently engaged with.

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.

The system is Screendoor.io, which is an open-source software designed to help government agencies be more efficient. Screendoor.io is open and free to the public. We have since contracted out IT services with the owners of Screendoor.io for technical support. The system is designed to house a 'catalog' of fellowship opportunities overseas with USAID science/technology/innovation/partnership countries, and it is available to select eligible Fellow groups. Currently this is confined to only NSF GRFP grant recipients, but it is anticipated that more

organizations/academic institutions will join this program to provide additional streams of Fellows. Ultimately the system will also be able to house the Fellows' resumes, so that they may easily (and voluntarily) send their information to potential hosting organizations. Additionally, it is anticipated that the system will expand to include a social networking/research collaboration feature that would be available only to Fellows, in order to share in-country experiences and learn from others' research.

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.)

<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 checked="" 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: 36T
<input type="checkbox"/> 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.)

<input type="checkbox"/> New System Development or Procurement
<input type="checkbox"/> Existing System Being Updated
<input type="checkbox"/> Existing Information Collection OMB Control Number: 36T
<input checked="" type="checkbox"/> New Data Collection Form or Survey
<input type="checkbox"/> Other: 36T
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.X
Yes: 36T
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: 36T

☐ Another Federal Agency: 36T

☐ Contractor: 36T

☐ Cloud Computing Services Provider: 36T

☒ Third-Party Website or Application Services Provider: Screendoor.io

☐ Mobile Services Provider: 36T

☐ Digital Collaboration Tools or Services Provider: 36T

☐ Other: 36T

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: 36T

☐ Application Developer: 36T

☐ Content Developer or Publisher: 36T

☐ Wireless Carrier: 36T

☐ Advertiser: 36T

☐ Equipment or Device Vendor: 36T

<input type="checkbox"/> Device User: 36T
<input type="checkbox"/> Internet Service Provider: 36T
<input type="checkbox"/> Third-Party Data Source (Data Broker): 36T
<input checked="" type="checkbox"/> Other: Screendoor.io
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.

- 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.

4. APPENDICES

4.1 APPENDIX A GLOSSARY

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

Table 4-1 Glossary

Abbreviations	Description
ADS	USAID Automated Directives System
Automated Directives System	
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)
D	Draft Version
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
Individual	A citizen of the United States or an alien lawfully admitted for permanent residence, as well as USAID employees and contractors.
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.

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 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.
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PO	Privacy Office
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, 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.
Privacy Threshold Analysis	An analysis used to determine whether a program uses PII and whether any privacy requirements apply to the program's collection, use, maintenance, and dissemination of PII.
PTA	Privacy Threshold Analysis
SORN	System of Records Notice
SP	NIST Special Publication
SSN	Social Security Number
System	For this purpose, 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.
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
Visitor to the United States	Someone who is not citizen of the United States or an alien lawfully admitted for permanent residence and who is visiting the United States legally.

4.2 APPENDIX B CONDUCTING THE PTA

4.2.1 Background

USAID is required to protect PII against anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained and to USAID. PTAs provide information on how programs handle PII, so that USAID employees and contractors will be able to fulfill their requirement to protect PII against unauthorized access or disclosure by ensuring that only those people who have a clearly demonstrated need to know or use the information are given access.

The PTA is a risk-based analysis that enables USAID to determine whether a particular program will encounter any privacy risks during the conduct of USAID business functions. The PTA process is designed to be a cross-cutting tool to address the requirements of several different privacy laws and policies. A PTA should be conducted initially for each USAID program and thereafter periodically and before developing or changing any program information process, including any new or updated information system or information collection.

This PTA 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 Analyst to analyze the privacy risks of the program.

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

4.2.2 Using this Word Template

This PTA 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 PTA electronically as an e-mail attachment. To create a PTA Word document from this PTA Template, use the following steps:

1. Click on **File** and then **Save As**.
2. In the **Save As** window save your PTA 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.

4.2.3 Completing the PTA Template

This PTA 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 section 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 Program Name field in the Header, and the Date field in the Footer. The date in the Footer should be the date you send this PTA to the Privacy Office for review.
- Update the Change History page to reflect your new version of this PTA. The date in the Change History should be the date you send this PTA 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 and System Owner.

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

4.2.4 Answering the Questions

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.
- Answer each question fully and completely. Answer each question with sufficient detail to permit the Privacy Office to analyze the possible privacy issues.
- 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 PTA.
- 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 PTA for approval.

4.2.5 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 D Privacy Controls ([hyperlink here](#)).

4.3 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 ([hyperlink here](#)).

Table 4-3 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 Data 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

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