Agency Secure Image and Storage Tracking System (ASIST) Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
Agency Security Image and Storage Tracking System (ASIST)
Approved Date: April 24, 2017

Additional Privacy Compliance Documentation Required:

☐ None

☐ System of Records Notice (SORN)

☐ Open Data Privacy Analysis (ODPA)

☐ Privacy Act Section (e)(3) Statement or Notice (PA Notice)

☐ USAID Web Site Privacy Policy

☒ Privacy Protection Language in Contracts and Other Acquisition-Related Documents

☐ Role-Based Privacy Training Confirmation

Possible Additional Compliance Documentation Required:

☐ USAID Forms Management. ADS 505

☐ Information Collection Request (ICR). ADS 505, ADS 506, and ADS 508 Privacy Program

☐ Records Schedule Approved by the National Archives and Records Administration. ADS 502

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). See **ADS 508 Privacy Program** Section 503.3.5.2 Privacy Impact Assessments.

2 Information

2.1 Program and System Information

2.1.1 Describe the PROGRAM and its PURPOSE.

The Office of the Chief Information Officer (M/CIO) is responsible for information resources management, as defined in the E-Government Act of 2002 and OMB Circular A-130, as well as for all Chief Information Officer functions mandated by the Clinger-Cohen Act of 1996.

The Information Technology Operations Division (M/CIO/ITO) is responsible for development, implementation, operation, and enhancement of enterprise business and infrastructure applications as per customer requirements as provided by the Engineering Branch. This division is also responsible for operating and maintaining USAID infrastructure and its components as well as USAID data administration functions.

The System Development Branch (M/CIO/ITO/SD) develops new business systems and applications, and executes the agency IT project life cycle methodology and establishes and maintains the project's life cycle documentation. The Branch also manages the Web Services that are accessed over the Internet, using standardized technologies and formats/protocols that simplify the exchange and integration of large amounts of data. It also manages unit testing, system testing, system integration testing, stress/volume testing and user acceptance testing, supports quality audits performed by Quality Management, and packages and distributes software for subsequent deployment by the Infrastructure/Operations Branch.

2.1.2 Describe the SYSTEM and its PURPOSE.

Agency Secure Image and Storage Tracking System (ASIST) is a content management solution. ASIST's user interface and functionality are a USAID custom front-end for Documentum, a software package. Documentum software provides centralized and generalized document storage and retrieval services relied on by system owners in USAID bureaus, offices, and missions in Washington and overseas missions. ASIST enables staff to track, search and access Agency documents that are stored in Documentum, such as correspondence, audit documents, payment documents and contract-related documents. The centralization, search capability, and access controls provided by ASIST and Documentum also facilitates Agency responses to Freedom of Information Act (FOIA), Privacy Act, and other disclosure requests. ASIST is customized and maintained by the USAID Office of the Chief Information Officer to improve the efficiency and security of handling documents for USAID Missions and Washington headquarters. USAID-specific customization includes direct support for folders and processes such as Correspondence, Contracts, Vouchers, SOs/Activities, and Personal Services Contracts. ASIST also enables the creation of custom folders to support other business processes and can incorporate desired index data without code changes.

ASIST makes available a variety of views that are available to provide close tracking and easy retrieval of stored documents. Search capabilities are available using full-text search on document contents and on attributes of the documents (metadata). For visual navigation, an Attribute Browser provides the ability to create and traverse

2.1.2 Describe the SYSTEM and its PURPOSE.

custom tree views providing a user friendly way of looking for folders. Customized workflows and folders can be implemented to support other business processes as required.

ASIST supports several business processes. Through Documentum, ASIST provides system owners with specific folders and workflows for USAID programs, including systems used by M/OAA and M/CFO. These systems include:

AADM: M/OAA uses ASIST to support the Acquisition and Assistance Document Management (AADM) system, which provides a standard file structure for storing all required files pertaining to contracts, task orders, and assistance agreements. This conforms to the most recent revision of the applicable Automated Directives System (ADS), as provided by M/OAA. Two new services and an automated process have been developed to provide automatic functions that integrate the Award folder type with the Global Acquisition and Assistance System (GLAAS). The services automatically query the GLAAS ODS database to identify certain changes to GLAAS requisition, solicitation, or award documents. In response to those changes, they create new Award folders, and update those folders, and existing Award folders, with the GLAAS awards metadata and with related GLAAS generated files. The process updates Award folder attachment types and user access for the folders.

CACS: M/CFO Audit Performance & Compliance Division (APC) uses ASIST to support the Consolidated Audit and Compliance System (CACS), which is an implementation within the ASIST application. CACS is designed to administer the agency's entire audit management, compliance, and reporting process. CACS allows users to track actions, submit requests for closure including supporting documentation, and print reports related to recommendations issued by USAID Office of Inspector General (OIG) and the Government Accountability Office (GAO). CACS also provides processes within ASIST to track actions for Federal Managers' Financial Integrity Act (FMFIA) Certifications, Corrective Action Plans (CAPs), Funds Control Violations (FCVs), Obligations Certifications, and Vendors Annual Audits. CACS is used by USAID Washington headquarters and missions.

TRACS: M/CFO/APC also uses ASIST to support the Tracking Audit Consolidated System (TRACS), which is used by action offices to manage and track annual vendor audits and other audits, surveys, reviews, procedures, and engagements.

Paperless Payments: M/CFO uses ASIST to support Paperless Payments, which provides electronic signature functionality within ASIST in accordance with USAID ADS policy. This electronic signature method has been approved by the Chief Information Security Officer and permits the use of ASIST document approvals in place of paper signatures when used appropriately.

ASIST is deployed to servers located in Terremark. The ASIST System consists of the following components: ASIST Web Application; Documentum Content Server and repository for content storage and workflow; and an Oracle database for storage of metadata. ASIST relies on the USAID PingFederate infrastructure for user authentication. The Oracle Database Administrators (DBAs) and Documentum Administrators provide the database instance and Documentum repository (or docbase) for use by ASIST. Each ASIST Administrator has appropriate access to maintain and update ASIST without intervention from Oracle DBAs or the Documentum Administrators, except in cases where there is a problem with the Oracle or Documentum software itself. Data is imported into ASIST from the PhoenixViewer application via parsing of flat files (Washington and missions) and direct database access (Washington-only). Data is imported into ASIST from the IG AIMS application via parsing of flat files (Washington-only). Data is imported into ASIST from GLAAS Operational Data Store (ODS) via direct database access (Washington-only).

The ASIST team will notify the Privacy Office if any of the information above changes. If additional USAID programs want to use ASIST or additional types of uses are contemplated, the ASIST Team will contact the Privacy Office immediately to consult on the risks and privacy concerns with the changes.

2.1.3 What is the SYSTEM STATUS?

☐ New System Development or Procurement

☐ Pilot Project for New System Development or Procurement

☒ Existing System Being Updated. (No technical updates, just completion of ASIST consolidation).

☐ Existing Information Collection Form or Survey
OMB Control Number:

☐ New Information Collection Form or Survey

☐ Request for Dataset to be Published on an External Website

☒ Other: Updated to new PIA template.

2.1.4 What types of INFORMATION FORMATS are involved with the program?

☐ Physical only
☐ Electronic only
☐ Physical and electronic combined

Documents and data are deposited into ASIST by a variety of means: 1) Electronic documents and data from GLAAS-ODS are automatically loaded into ASIST (beginning with ASIST 3.10) by a nightly process. 2) Hardcopy paper documents are scanned using scan software and are then loaded into ASIST typically as PDF files. 3) Other electronic documents are added manually by users who employ the Drag & Drop or Add File function. 4) Electronic data from IG AIMS is automatically loaded into ASIST by a nightly process. 5) Electronic data from PhoenixViewer is automatically loaded into ASIST by a nightly process. 6) Documents can be emailed to other users from within ASIST and can be sent through a workflow process. 7) Electronic signature within ASIST is supported for the M/CFO voucher approval process. Documents stored within ASIST are opened in their native application for viewing (i.e. Word, Excel, Adobe Acrobat). Once opened in the native application the document ca be printed if desired.

2.1.5 Does your program participate in PUBLIC ENGAGEMENT?

☒ No.

☐ Yes:
- ☒ Information Collection Forms or Surveys
- ☐ Third Party Web Site or Application
- ☐ Collaboration Tool

2.1.6 What type of system and/or TECHNOLOGY is involved?

☒ Infrastructure System (Local Area Network, Wide Area Network, General Support System, etc.)

☒ Network

☒ Database

☒ Software

2.1.6 What type of system and/or TECHNOLOGY is involved?
☒ Hardware
☐ Mobile Application or Platform
☐ Mobile Device Hardware (cameras, microphones, etc.)
☐ Quick Response (QR) Code (matrix geometric barcodes scanned by mobile devices)
☒ Wireless Network
☐ Social Media
☐ Web Site or Application Used for Collaboration with the Public
☐ 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:
☐ None

2.1.7 About what types of people do you collect, use, maintain, or disseminate personal information?
☒ Citizens of the United States
☒ Aliens lawfully admitted to the United States for permanent residence
☒ USAID employees and personal services contractors
☒ Employees of USAID contractors and/or services providers

2.1.7 About what types of people do you collect, use, maintain, or disseminate personal information?
☒ Aliens
☒ Business Owners or Executives
☐ Others:
☐ None

2.2 Information Collection, Use, Maintenance, and Dissemination

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☒ 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
☒ Criminal Record

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☒ Military Record
☒ Financial Record
☒ Education Record
☒ Biometric Record (signature, fingerprint, photo, 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:
☐ No PII is collected, used, maintained, or disseminated

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☒ 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

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☐ Audio or Sound Data
☐ Other Device Sensor Controls or 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:
☒ None

2.2.4 Who owns and/or controls the system involved?
☒ USAID Office: M/CIO
☐ Another Federal Agency:
☐ Contractor:
☒ Cloud Computing Services Provider:
☐ Third-Party Website or Application Services Provider:
☐ Mobile Services Provider:
☐ Digital Collaboration Tools or Services Provider:
☐ Other:

3 Privacy Risks and Controls

3.1 Authority and Purpose (AP)

3.1.1 What are the statutes or other LEGAL AUTHORITIES that permit you to collect, use, maintain, or disseminate personal information?

5 USC 301, Departmental Regulations; 22 U.S.C. Ch. 32, Foreign Assistance, Subchapter I, International Development; 5 U.S.C. Part III, Employees, Subpart D, Pay and Allowances; 22 U.S.C. Ch. 14, Foreign Service, Subchapter I, General Provisions; 22 U.S.C. Ch. 52, Foreign Service, Subchapter IV, Compensation; 26 U.S.C. 6109, Identifying numbers; 31 U.S.C. 3512, Executive agency accounting and other financial management reports and plans, and 3513, Financial reporting and accounting system; 42 U.S.C. 659, Consent by United States to income withholding, garnishment, and similar proceedings for enforcement of child support and alimony obligations; 44 U.S.C. 3101, Records management by agency heads; general duties; Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons, 3 CFR, 1943-1948 Comp., p. 283, as amended by E.O. 13478, Amendments To Executive Order 9397 Relating To Federal Agency Use of Social Security Numbers, 73 FR 70279 (Nov. 18, 2008).

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

ASIST is an electronic document management system (Documentum) that supports USAID systems by providing an environment for storage of information and documentation that the system needs to perform its function. ASIST allows system owners to track, search, and access various types of documents stored in ASIST. These documents can contain various elements of PII, including names, addresses, telephone and fax numbers, e-mail addresses, financial information such as bank account information, credit information, and Social Security numbers. A recent cursory search of the ASIST environment indicated that the information stored by system owners might include medical information. Whether the medical information is identifiable is unknown.

The functions of the systems supported by ASIST include contract, financial (procurement and contracts management), audit, and personnel functions (payroll, personal services contracting, and travel authorizations, correspondence, and audits of USAID.

3.1.3 How will you identify and evaluate any possible new uses of the PII?

USAID programs are authorized to useASIST to manage records. The programs are responsible for identifying and evaluating any possible new uses of the records. Any new uses would be documented in the individual SORNs for the specific program records, as follows:

USAID-1 Foreign Service Personnel Records
USAID-16 Time, Attendance and Payroll
USAID-17 Employee Owned or Leased Property Records
USAID-18 Employee Use of Property Owned or Leased by the US Government Records
USAID-21 Public Information Records
USAID-22 Congressional Relations, Inquiries, & Travel Records
USAID-33 Phoenix
USAID-34 Personal Services Contracts

OPM/Gov-1 General Personnel Records

3.2 Accountability, Audit, and Risk Management (AR)

3.2.1 Do you use any data collection forms or surveys?

☒ No:

☐ Yes:

- ☐ Form or Survey (Please attach)
- ☐ OMB Number, if applicable:
- ☐ Privacy Act Statement (Please provide link or attach PA Statement)

3.2.3 Who owns and/or controls the personal information?

☒ USAID Office:

☐Another Federal Agency:

☒ Contractor: Team IBM

☒ Cloud Computing Services Provider: Terremark, Miami, FL

☐ Third-Party Web Services Provider:

☐ Mobile Services Provider:

☐ Digital Collaboration Tools or Services Provider:

☐ Other:

3.2.8 Do you collect PII for an exclusively statistical purpose? If you do, how do you ensure that the PII is not disclosed or used inappropriately?

☒ No.

☐ Yes:

3.3 Data Quality and Integrity (DI)

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

The USAID programs authorized to use ASIST have control over the processes for collecting PII from individuals. See the appropriate SORN below for specific information on records sources:
USAID-1 Foreign Service Personnel Records
USAID-16 Time, Attendance and Payroll
USAID-17 Employee Owned or Leased Property Records
USAID-18 Employee Use of Property Owned or Leased by the US Government Records
USAID-21 Public Information Records
USAID-22 Congressional Relations, Inquiries, & Travel Records
USAID-33 Phoenix
USAID-34 Personal Services Contracts
OPM/Gov-1 General Personnel Records

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

ASIST is a document management system that maintains agency documents already collected or generated in the course of agency business. Accordingly, these documents are placed into the system "as is" without verifying their accuracy or timeliness. The accuracy and timeliness of the information in such documents is verified, however, as necessary and appropriate at the time they are collected, used, or disseminated.

The ASIST SO does not manage this and relies on the user programs responsible for the initial collections. The USAID programs authorized to use ASIST have the responsibility for ensuring that the PIII is accurate, relevant, timely, and complete at the time of collection. Program Managers must validate PII that is obtained from sources other than the subject individuals or the authorized representatives of such individuals. This is necessary to assure fairness in any determination about an individual. The PII in this system is collected directly from the subject individual to the greatest extent possible. See the appropriate SORN below for specific information:

USAID-1 Foreign Service Personnel Records
USAID-16 Time, Attendance and Payroll
USAID-17 Employee Owned or Leased Property Records
USAID-18 Employee Use of Property Owned or Leased by the US Government Records
USAID-21 Public Information Records
USAID-22 Congressional Relations, Inquiries, & Travel Records
USAID-33 Phoenix
USAID-34 Personal Services Contracts
OPM/Gov-1 General Personnel Records

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

ASIST is a document management system that maintains agency documents already collected or generated in the course of agency business. Accordingly, these documents are placed into the system "as is" without verifying their accuracy or timeliness. ASIST is not involved in the determination on how long documents are maintained or whether documents are retired from ASIST. The USAID programs authorized to use ASIST verify, periodically as necessary and appropriate, the accuracy and timeliness of the information in such documents.

3.4 Data Minimization and Retention (DM)

3.4.1 What is the minimum PII relevant and necessary to accomplish the legal purpose of the program?

The USAID programs authorized to use ASIST determine the minimum PII relevant and necessary. All uses of the data are relevant and necessary to the purpose for which it was collected, as shown in the appropriate SORN below for specific programs:

USAID-1 Foreign Service Personnel Records
USAID-16 Time, Attendance and Payroll
USAID-17 Employee Owned or Leased Property Records
USAID-18 Employee Use of Property Owned or Leased by the US Government Records
USAID-21 Public Information Records
USAID-22 Congressional Relations, Inquiries, & Travel Records
USAID-33 Phoenix
USAID-34 Personal Services Contracts

OPM/Gov-1 General Personnel Records

3.4.3 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?

☒ No.

☐ Yes:

3.4.4 What types of reports about individuals can you produce from the system?

ASIST can provide reports based on the ASIST folder information which is collected and stored as discrete data elements in the database, such as “Contract number”, “Due Date”, etc. ASIST does not store specific information about individuals in these discreet data elements.

In the Advanced Search tool in ASIST, users can build queries to retrieve information based on these discrete ASIST data elements such as Contract Number=1123 or Due Date = 01/15/15. These data elements will then appear in the search results, if the user has access. The user can open the folders listed in the search results directly on the results screen in ASIST or the results list can be exported to an MS Excel or PDF file.

Users can also search for text that appears anywhere in documents stored in ASIST (such as MS Office and searchable PDF documents) by adding criteria in the “Add Text to Search For” option in the Advanced Search tool. Folders which contain documents containing the search term will then appear in the search results, if the user has access. However, neither the text search term, nor the location in the document will appear in the search result. The search results still only display the discrete data elements from the ASIST folder. In this case, a user could perform a text search on a person’s Name or other information; however that information will not directly appear in the search results.

ASIST Administrators may periodically query the ASIST database for the user names of ASIST user accounts in order to fulfill FISMA audit requirements. ASIST user account information only contains work-related information such as the User Name, work address, and work email address.

3.4.6 Does the system monitor or track individuals?

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

☐ No.

☒ Yes: ASIST monitors and tracks users to provide access management and control for the various programs that use ASIST for document management.

3.5 Individual Participation and Redress (IP)

3.5.1 Do you contact individuals to allow them to consent to your collection and sharing of PII?

The USAID programs authorized to use ASIST have control over the processes for consent. For those programs that collect information directly from the subject individual, the program includes a Privacy Act Statement at the point of collection, per Privacy Act section (e)(3). See the following appropriate SORN for more information:

USAID-1 Foreign Service Personnel Records
USAID-16 Time, Attendance and Payroll
USAID-17 Employee Owned or Leased Property Records
USAID-18 Employee Use of Property Owned or Leased by the US Government Records
USAID-21 Public Information Records
USAID-22 Congressional Relations, Inquiries, & Travel Records
USAID-33 Phoenix
USAID-34 Personal Services Contracts

OPM/Gov-1 General Personnel Records

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

ASIST provides no additional mechanism beyond the Privacy Act and FOIA request processes.

3.5.3 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 to and amendment of their PII?

The Cloud Computing Service Terremark provides hosting for USAID's data center. However the data stored within the ASIST application remains available to the USAID programs authorized to use ASIST and collect such information.

3.7 Transparency (TR)

3.7.1 Do you retrieve information by personal identifiers, such as name or number?

(If you choose Yes, please provide the types of personal identifiers that are used.)

☐ No.

☒ Yes: For example, records related to personal services contracts; correspondence; personnel management; and time, attendance, and payroll are accessed by name of the individual involved.

3.7.2 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:

4) The effects on the individual, if any, of not providing all or any part of the PII:

There are several SORNs that provide notice to the public about records in ASIST:

USAID-1 Foreign Service Personnel Records

USAID-16 Time, Attendance, and Payroll

USAID-17 Employee Owned or Leased Property Records

USAID-18 Employee Use of Property Owned or Leased by the US Government Records

USAID-21 Public Information Records

USAID-22 Congressional Relations, Inquiries, & Travel Records

USAID-33 Phoenix

USAID-34 Personal Services Contracts Records

OPM/Govt-1 General Personnel Records

3.7.3 Is there a Privacy Act System of Records Notice (SORN) that covers this system?

☐ No

☒ Yes: There are several SORNs that cover records in ASIST:

USAID-1 Foreign Service Personnel Records

USAID-16 Time, Attendance, and Payroll

USAID-17 Employee Owned or Leased Property Records

USAID-18 Employee Use of Property Owned or Leased by the US Government Records

USAID-21 Public Information Records

3.7.3 Is there a Privacy Act System of Records Notice (SORN) that covers this system?

USAID-22 Congressional Relations, Inquiries, & Travel Records

USAID-33 Phoenix

USAID-34 Personal Services Contracts Records

OPM/Govt-1 General Personnel Records

3.7.4 If your system involves cloud computing services, 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?

The contract with Terremark specifies that the Terremark Private Cloud hosting environment will be at Terremark's Miami, FL data canter.

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

The USAID personnel of the programs that use ASIST and support contractors to these programs have access to ASIST. All USAID program personnel and contractors with access to the system can do so at a read-only permission level. Access to documents and their metadata is further restricted based on a need to know.

CIO personnel and contractors providing system administration support have access to ASIST. The M/CIO system administrator and contractors who support the system administrator have full access rights to all documents and metadata in the system in order to assist with maintenance of and enhancements to the system and, in some instances, content management.

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

There are a variety of ASIST systems used in USAID offices worldwide. ASIST does not restrict authorized users from sending information to which they have access outside of USAID. Further, ASIST does not restrict to whom the information is sent. Such determinations are made by the programs that use ASIST to manage the documents related to their functions. All information that is sent outside of ASIST is recorded in an audit record.

The following SORNs explain with whom specific types of records might be shared and for what purposes:

USAID-1 Foreign Service Personnel Records

USAID-16 Time, Attendance, and Payroll

USAID-17 Employee Owned or Leased Property Records

USAID-18 Employee Use of Property Owned or Leased by the US Government Records

USAID-21 Public Information Records

USAID-22 Congressional Relations, Inquiries, & Travel Records

USAID-33 Phoenix

USAID-34 Personal Services Contracts Records

OPM/Govt-1 General Personnel Records

3.8.4 Do you share PII outside of USAID? If so, 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?

☐ No.

☒ Yes: The USAID programs that use ASIST have control over the sharing of PII outside of USAID. The following SORNS explain with whom specific types of records might be shared and for what purposes. The System of Records Manager is responsible for ensuring the accuracy of the SORN, and any changes require the System of Records Manager to alter the appropriate SORN in consultation with the Privacy Office.

USAID-1 Foreign Service Personnel Records

USAID-16 Time, Attendance, and Payroll

USAID-17 Employee Owned or Leased Property Records

USAID-18 Employee Use of Property Owned or Leased by the US Government Records

USAID-21 Public Information Records

USAID-22 Congressional Relations, Inquiries, & Travel Records

USAID-33 Phoenix

USAID-34 Personal Services Contracts Records

OPM/Govt-1 General Personnel Records

3.9 Third-Party Web Sites and Applications

3.9.1 What PII *could be made available* (even though not requested) to USAID or its contractors and service providers when engaging with the public?

Not applicable.

Appendix A. Links and Artifacts

A.1 Privacy Compliance Documents or Links

☐ None. There are no documents or links that I need to provide.
☐ Privacy Threshold Analysis (PTA)
☒ Privacy Impact Assessment (PIA) https://www.usaid.gov/privacy-policy/pia-summaries
☒ System of Records Notice (SORN) https://www.usaid.gov/privacy-policy/systems-records-notices-sorns
☐ Open Data Privacy Analysis for Posting Datasets to the Public (ODPA)
☐ Data Collection Forms or Surveys
☐ Privacy Act Section (e)(3) Statements or Notices
☐ USAID Web Site Privacy Policy
☐ Privacy Policy of Third-Party Web Site or Application
☐ Privacy Protection Language in Contracts and Other Acquisition-Related Documents