Global Acquisitions and Assistance System (GLAAS)

Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

<div align="right">

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
[ITIS/GLAAS]
Approved Date: April 3, 2017

</div>

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 Acquisition and Assistance (OAA) operates the Global Acquisition and Assistance System (GLAAS), a procurement system that supports acquisition and assistance management by automating all aspects of the procurement life cycle, including procurement planning, requisition, solicitation/funding opportunity, award, and closeout. GLAAS is an agency-wide implementation of a web-based, commercial off-the-shelf (COTS) procurement solution.

2.1.2   Describe the SYSTEM and its PURPOSE.

GLAAS is an initiative by the United States Agency for International Development (USAID) that supports the Agency's Acquisition and Assistance (A&A) management life cycle. GLAAS provides support for end-to-end A&A business processes performed by a wide variety of agency staff, from the development of the requisition, solicitation or funding opportunity, award, and award closeout. GLAAS pulls data from two systems of record only – Phoenix and SAM.

To maximize the efficiency of the agency staff, GLAAS provides automated interfaces with other systems that are critical to the A&A processes. GLAAS interfaces with:

1. Phoenix, the Agency Financial Management System to process commitments and obligations associated with A&A actions.
2. FedConnect and FedBizOps to post procurement business opportunities and receive proposals.
3. Grants. gov to post synopses for funding opportunities for assistance.
4. The Federal Procurement Data System – Next Generation (FPDS-NG) to post acquisition awards information.
5. ASIST to post contract files.
6. The Federal Assistance Award Data System (FAADS/FAADS Plus) to post grant and cooperative agreement award information.

GLAAS has existing MOUs and information sharing agreements (ISAs) with these systems.

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
☐ 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:

2.1.4   What types of INFORMATION FORMATS are involved with the program?
☐ Physical only ☒ Electronic only ☐ Physical and electronic combined

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
☒ 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

2.1.6   What type of system and/or TECHNOLOGY is involved?
☐ 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: IaaS at Terremark
☐ 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
☐ Aliens
☐ Business Owners or Executives
☒ Others: Vendors (whether businesses or people)
☐ 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 (some vendors name their business entities after themselves).
☐ 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
☐ Military Record
☐ Financial Record
☐ Education Record
☐ Biometric Record (signature, fingerprint, photo, voice print, physical movement, DNA marker, retinal scan, etc.)
☐ Sex or Gender
☐ Age

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

☐ 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
☐ 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

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☐ 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: Management Bureau, Office of Acquisition and Assistance (M/OAA)
☐ Another Federal Agency:
☒ Contractor: Under M/CIO, IT IS Contract under M/CIO supports the system.
☐ 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?
22 U. S. C. 2381 (Section 621 of the Foreign Assistance Act of 1961); OMB Circular A-110 .

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

GLAAS collects contract/procurement information (purchase orders, contracts and grants) as well as name of vendors (personal service contractors). This would include vendor data, shipping data, items/services purchased and costs. The information is used in a business capacity to identify the vendor that has been awarded a purchase order, contractor grant and to process payment.

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

Any proposed new uses of PII in GLAAS will first be evaluated against the existing uses in the source system SORNs and other privacy documentation. Any new uses of PII will be contrasted against the purpose of this system to ensure the relevant policy gaps are filled.

Release notes from the vendor and any changes to the system or use of its data shall be reviewed by the application O&M CCB to ensure compliance with Agency policy in any new uses of PII.

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: Management Bureau, Office of Acquisition and Assistance (M/OAA)

☐ Another Federal Agency:

☐ Contractor:

☐ Cloud Computing Services Provider:

☐ 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?
Phoenix (77 FR 73973) receives its vendor data from SAM (78 FR 11648) which is the main system of record for all government contractors. GLAAS collects PII through an electronic feed from Phoenix. The MOU with Phoenix and Information Sharing Agreement (ISA) with SAM cover the use of SAM data in GLAAS.	

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?
SAM and Phoenix are the relevant systems of record. The information in SAM and Phoenix is validated at the point of collection and is then fed from Phoenix and SAM into GLAAS. GLAAS pulls data from Phoenix every two hours.	

3.3.3	How do you check for, and correct as necessary, any inaccurate or outdated PII in the system?
SAM and Phoenix are the relevant systems of record. The information in SAM and Phoenix is validated at the point of collection and is then fed from Phoenix and SAM into GLAAS Additionally, GLAAS pulls data from Phoenix every two hours.	

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?
Entity name, entity address, first name, and last name (in cases where individuals name their business entities after themselves), and address. This information is used to contact the recipient/vendor when issuing an award in GLAAS.	

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?

GLAAS reports involve all aspects for the procurement lifecycle (procurement planning, requisition, solicitation/funding opportunity, award and closeout).

Reports may include vendor name and contact information (business address, work phone, cell phone, business email) in addition to status information on the procurement. Individuals would only be listed if they were a vendor to USAID. Admin reports are only accessible to the seven system admins. The other reports are controlled by user role. The reports are for the internal USAID use only and not for distribution outside USAID. Each report is marked with a Sensitive But Unclassified (SBU) marking.

3.4.6   Does the system monitor or track individuals?

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

☒ No.

☐ Yes:

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?

No. Vendors submit their data to SAM in order to do business with the Agency. SAM feeds data to Phoenix and Phoenix, in turn, feeds GLAAS.

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?

The relevant system of records to access or amend is SAM, a vendor management system that feeds Phoenix which in turn feeds GLAAS. Individuals can contact the system of records owner listed in the SAM SORN.

Updated data is pulled from SAM via Phoenix into GLAAS every two hours. Modifications to the contract can be created to update the information as needed in a separate contract modification document.

Individuals may also contact USAID regarding data in the Phoenix system (see 3. 7. 3). Additional assistance is provided by the federal service desk at https://www. fsd. gov/fsd-gov/home. do.

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?

GLAAS does not involve cloud computing services.

Vendors update the vendor system of record (SAM). Phoenix then pulls the vendor updates from SAM. GLAAS pulls the vendor updates from Phoenix. All changes to vendor data are made through SAM and propagate to GLAAS.

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: Information can be retrieved by vendor's entity name, or Data Universal Number (DUNS Number).

3.7.2	How do you provide notice to individuals regarding?

1) The authority to collect PII: SAM SORN (78 FR 11648) and the Phoenix SORN (77 FR 73973).

2) The principal purposes for which the PII will be used: Principal purposes are described in the SAM SORN (78 FR 11648) and the Phoenix SORN (77 FR 73973.

3) The routine uses of the PII: Routine uses are described in the SAM SORN (78 FR 11648) and the Phoenix SORN (77 FR 73973).

4) The effects on the individual, if any, of not providing all or any part of the PII: Individuals or entities that do not provide contact information will not be able to do business with the US Government.

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

☐ No

☒ Yes: SAM - 78 FR 11648; Phoenix - 77 FR 73973

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?

GLAAS is currently in the Terremark co-location environment which are physical servers owned by USAID. System locations are covered in the system of record notices for SAM (78 FR 11648) and Phoenix (77 FR 73973).

3.8   Use Limitation (UL)

3.8.1   Who has access to the PII at USAID?
1. GLAAS System Administrators 2. Contracting Officers 3. GLAAS users within the originating Bureau or Mission (Requestors, Program Officers, Agreement Officers, Contracting Officers Representative (CORs) and; 4. Agreement Officers Representative (AORs), Negotiators, Program Manager and Financial Management Officers (FMOs)). All roles (except System Administrators and Contracting Officers) are restricted to the office to which they belong. This is validated by the user's supervisor.

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?
No PII is shared outside of USAID.

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. PII is not shared outside of USAID. ☐ Yes:

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?
NA

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)
☐ System of Records Notice (SORN)
☐ 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