General Support System (OIGNet)

Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
Office of Inspector General/OIGNet
Approved Date: November 23, 2016

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 United States Agency for International Development (USAID) is the lead U.S. Government agency that works to end extreme global poverty and enable resilient, democratic societies to realize their potential. The USAID mission states: We partner to end extreme poverty and promote resilient, democratic societies while advancing our security and prosperity.

USAID Office of Inspector General's (OIG) oversight of USAID, the Millennium Challenge Corporation (MCC), the United States African Development Foundation (USADF), the Inter-American Foundation (IAF), and the Overseas Private Investment Corporation (OPIC) helps ensure that the foreign assistance programs delivered by these agencies provide the aid needed around the world while also protecting U.S. taxpayers' interests. The OIG's mission is to protect and enhance the integrity of U.S. foreign assistance programs and operations administered by USAID, USADF, IAF, MCC, and OPIC. In its mission, OIG helps shape the success or failure of agency programs by assessing and recommending improvements in program planning, implementation, monitoring, and performance, as well as by working to detect and deter fraud, waste, and abuse.

OIGNet is the General Support System (GSS) for USAID Office of Inspector General (USAID/OIG), supporting all non-classified information technology needs for USAID/OIG globally. OIGNet, as the primary IT infrastructure and computing environment for USAID/OIG, provides network infrastructure, servers, workstations, telecommunications, identity and access management and related supporting functions.

OIGNet also provides hosting for applications, virtualized machines for hosting, data- and tele- communications connectivity (including remote access) and a variety of USAID/OIG mission critical applications. These resources support the USAID/OIG's automated business processes for Auditing, Investigation, and Management Divisions, to include financial and information security audits, criminal investigations, budgeting, planning, procurement, contracts monitoring and awards, tracking results and performance, and administrative functions.

2.1.2 Describe the SYSTEM and its PURPOSE.

OIGNet is comprised of the ig.usaid.gov domain and the oigres.gov forest. The ig.usaid.gov domain is a child domain of the United States Agency for International Development (USAID) General Support System (AIDNet). System Administrators of AIDNet manage USAID enterprise resources in the ig.usaid.gov domain, such as e-mail and domain controllers. Oigres.gov is a separate domain for OIG applications and data and is logically segregated from AIDNet. The ig.usaid.gov domain is used by USAID/OIG for external resources including e-mail, corporate applications, and Internet/Intranet access. USAID/OIG administrators have restricted Administrator rights to the ig.usaid.gov domain. The oigres.gov domain is not trusted by any domain, but has a one-way trust relationship with ig.usaid.gov domain utilizing user assigned permissions. The oigres.gov forest houses OIG resources. USAID/OIG administrators have full administrator rights in the oigres.gov forest.

2.1.2 Describe the SYSTEM and its PURPOSE.

USAID/OIG users may access OIGNet by logging into the ig.usaid.gov domain from workstations connected to AIDNet. Remote access to OIGNet is available to users located in overseas Regional Inspectors General offices, and to telecommuters, via Citrix, which is available with any Internet connect and secured through a two-factor authentication. The system utilizes a continuous replication process to backup data and domain controllers. Data transfers are encrypted using AES 256-bit encryption.

The OIGNet COOP Site contains the hot backups of vital USAID/OIG systems and replicated data. Backup tapes are also maintained for vital USAID/IG data.

The OIGNet, rated Mission-Critical, is located in the Ronald Reagan Building, the Millennium Challenge Corporation offices in Washington DC, overseas at the Regional Inspector General offices, and the Terremark Data Center in Miami Florida. Terremark provides only the physical storage facility for the servers. USAID OIG owns the servers on which this system operates, and USAID OIG network staff accesses the facility to maintain the servers. No server maintenance work is performed by contactors. OIG segregates its servers and the information thereon from other AID servers.

Currently, the systems audit logs are manually reviewed by OIGNet security staff on a monthly basis. However, OIG plans to automate the review process, in part, and anticipates implementing software that will scan audit log data, identify irregularities and suspicious activity, and notify responsible parties for appropriate attention.

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: User Access Request Forms (OIG Form 5006A) for new users and the Active Directory Database. Form 5006A requests a person's name, title, office, work location, employment type (federal or contractor) and company name. The form is handled by HR staff, the employee's supervisor, and IT staff for processing, and it is physically stored in a locked cabinet when not used.

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
☐ 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

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

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☒ 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
☐ 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): OIG uses Hyena software, which logs user names, the date of account creation, password changes and expiration dates, logins, account type, mailbox account details, and directory access details. No access log is generated by OIGNet.
☐ Tracking Data (single- or multi-session cookies, beacons)
☐ Form Data
☐ User Names
☒ Passwords
☒ Unique Device Identifier: USAID machine number and VPN for mobile devices.
☐ 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
☐ 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: USAID/OIG owns OIGNet, which is maintained by the OIG/M/Information Management (IM) division. System Management of OIGNet is shared between the USAID/IG/M/IM and USAID/M/CIO. The oigres.gov domain is managed by System Administrators from USAID/IG/M/IM, while the oigres.gov is managed by System Administrators from USAID/M/CIO and USAID/IG/M/IM.

☐ 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, Subchapter I, Foreign Assistance Act of 1961, as amended.

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

OIGNet does not collect and use PII, but provides the network infrastructure upon which other USAID/OIG systems rely for an operating environment. These systems can collect PII and, pursuant to the E-Government Act and OMB guidance, are each covered by their own separate system documentation, such as PTAs and PIAs.

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

OIGNet does not use PII, but provides the infrastructure for other USAID/OIG systems that are responsible for the PII. These systems that collect PII using the OIGNet infrastructure are covered by their own separate PIAs.

3.2 Accountability, Audit, and Risk Management (AR)

3.2.1 Do you use any data collection forms or surveys?

☒ No: OIGNet does not use data collection forms or surveys. Some systems hosted on OIGNet use data collection forms. These systems that collect PII using the OIGNet infrastructure are covered by their own separate PIAs.

☐ 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: USAID/OIG

☐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?

OIGNet does not collect PII, but provides the infrastructure for other USAID/OIG systems that are responsible for the PII. These systems that collect PII using the OIGNet infrastructure are covered by their own separate PIAs.

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?

USAID/IG/M/ Information Management (IM) collects PII from new users via the User Access Request Form (OIG Form 5006A). The users are required to present in person to the Office of Security two forms of government-issued identifications to verify their identity.

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

Contractors are required to undergo an annual re-badging, which requires them to verify in person their identity to the Office of Security, using two forms of government-issued identifications to verify their identify to include their name. OIGNet is a means of storage (and transmission) that supports other USAID Federal information systems. As such, only the System Owners and ISSOs whose systems use OIGNet can respond to queries regarding the timeliness and updating of inaccurate PII for their respective systems.

OIGNet is a means of storage (and transmission) that supports other USAID Federal information systems. As such, only the System Owners and ISSOs whose systems use OIGNet can respond to queries regarding the timeliness and updating of inaccurate PII for their respective systems.

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?

OIGNet collects at a minimum the name, and work telephone number for the purpose of OIGNet account management. It is a means of storage that supports other USAID Federal information systems. As such, the risks to PII are assessed, analyzed, and managed by the System Owners and ISSOs for each system, including the risk that collection of PII is excessive.

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?

No reports about individuals are produced by OIGNet.

3.4.6 Does the system monitor or track individuals?

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

☐ No.

☒ Yes: OIGNet monitor and track users to provide access management and control for USAID/OIG systems. A log of OIGNet users activities, such a log on, and log off, are recorded and stored in Active Directory.

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?

USAID/OIG system owners and program managers are responsible for the proper collection, use, maintenance, of PII in the specific systems that use the OIGNet infrastructure. The systems that collect, maintain and store PII using the OIGNet infrastructure are covered by their own separate PIAs.

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?

USAID/OIG system owners and program managers are responsible for the proper collection, use, maintenance, of PII in the specific systems that use the OIGNet infrastructure. The systems that collect, maintain and store PII using the OIGNet infrastructure are covered by their own separate PIAs.

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?

No applicable. OIGNet does not include any cloud computing services.

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:

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:

Not applicable. OIGNet does not collect or use PII.

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

☒ No. OIGNet is a general support system and a network. OIGNet hosts other applications, which may collect PII.

These applications exist on the OIGNet platform and the collection and legitimate handling of PII is addressed in those separate applications' PIAs and SSPs. Users cannot use the applications without authenticating into OIGNet. OIGNet does not possess or control any PII that is not within boundaries of the applications within its platform. Thus, no SORN is required.

☐ Yes:

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?

Not applicable. OIGNet does not include cloud computing services.

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

USAID/OIG system owners and program managers are responsible for the proper collection, use, maintenance, of PII in the specific systems that use the OIGNet infrastructure. The systems that collect, maintain and store PII using the OIGNet infrastructure are covered by their own separate PIAs. Specifically for OIGNet, only the USAID/IG Helpdesk privileged users have logical access to the PII contained in Active Directory, on the Domain Controllers.

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?

USAID/OIG system owners and program managers are responsible for the proper collection, use, maintenance of PII in the specific systems that use the OIGNet infrastructure. The systems that collect, maintain and store PII using the OIGNet infrastructure are covered by their own separate PIAs.

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. USAID/OIG system owners and program managers are responsible for the proper collection, use, maintenance, of PII in the specific systems that use the OIGNet infrastructure. The systems that collect, maintain and store PII using the OIGNet infrastructure are covered by their own separate PIAs. The PII collected and accessed for OIGNet is strictly for the purpose of Account Management. This PII is stored in Active Directory on the Domain Controllers, which can only be accessed by the USAID/IG/M/ Information Management (IM) Helpdesk privileged users. Terremark, which provides the infrastructure to host the OIGNet alternate processing site, does not have logical access to OIGNet Domain Controllers, which stores the PII. The PII is stored encrypted on the Domain Controllers.

☐ 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?

USAID/OIG system owners and program managers are responsible for the proper collection, use, maintenance, of PII in the specific systems that use the OIGNet infrastructure. The systems that collect, maintain and store PII using the OIGNet infrastructure are covered by their own separate PIAs.

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