AIDNet Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
AIDNet
Approved Date: August 8, 2014

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 (IRM), 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, including performing systems acquisition, development, and integration. The IT Operations Division (M/CIO/ITO) is responsible for “development, implementation, operation, and enhancement of enterprise business and infrastructure applications as per customer requirement s 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 Infrastructure/Operations Branch (M/CIO/ITO/IO) provides IT infrastructure implementation, integration, testing and deployment. It operates and maintains USAID IT operations and production systems including overall General Support System (GSS), Wide Area Network/Local Area Network (WAN/LAN), Internet Service Provider (ISP) connectivity, network services (remote access, Blackberry, voice over IP, video teleconferencing, etc.), and e-mail servers, and supports the areas of IT infrastructure and software administration, incremental upgrades, and patch upgrades . In addition, the Branch maintains the production lab and i-lab environments for the management and support of existing and new IT systems and conducts Operational Readiness Reviews for all new systems and infrastructure changes before release into production environments.

2.1.2 Describe the SYSTEM and its PURPOSE.

This PIA covers AIDNet, ALLNet, DEVNet, DMZ, and Wireless services. AIDNet and Wireless services that transport data and provide file storage. DMZ provides security services; it does not process data. ALLNet provides collaboration and communication services, and DEVNet provides a protected location for systems development, testing, and research.

2.1.2 Describe the SYSTEM and its PURPOSE.

AIDNet: AIDNet is the General Support System (GSS) for US Agency for International Development, supporting all non-classified information technology needs for USAID globally. This GSS supports the Agency's capability to provide foreign assistance in over I00 countries to: promote broadly shared economic prosperity; strengthen democracy and good governance; improve global health, food security, environmental sustainability and education; help societies prevent and recover from conflicts; and provide humanitarian assistance in the wake of natural and man-made disasters. To support that mission, AIDNet provides network infrastructure, servers, workstations, telecommunications, access management, and related supporting functions. AIDNet is an enterprise-level GSS providing a wide range of capabilities in challenging mission environments worldwide, including, for example, during hostile engagements, difficult geographies, and in climatic or meteorological disasters.

AIDNet is the primary IT infrastructure and computing environment for USAID. It provides hosting for applications, virtualized machines for hosting data and telecommunications connectivity (including remote access) and a variety of mission critical applications. These resources support the Agency's automated business processes for budgeting, planning, procurement, contracts monitoring and awards, tracking results and performance, and administrative functions. AIDNet either hosts or facilitates functionality for critical USAID systems. System owners and program managers are responsible for the proper collection, use, maintenance, and dissemination of PII in specific systems that use AIDNet infrastructure. The systems using AIDNet infrastructure that collect, use, maintain, or disseminate PII are covered by their own separate Privacy Impact Assessments (PIAs). The infrastructure for these systems is covered in this PIA, which includes PII protection during transfer within USAID and between USAID and outside systems, and PII protection at rest in shared and local storage. PII protection during use by a USAID system is covered by the individual PIA for the specific system.

Information is stored in AIDNet in centralized storage (shared drives), as well as local storage on servers and user-dedicated systems. System owners and program managers of specific systems that use ALLNet infrastructure are responsible for the proper collection, use, maintenance, and dissemination of PII in centralized and local storage locations. The systems using ALLNet infrastructure that collect, use, maintain, or disseminate PII are covered by their own separate PIAs. In additional, USAID personnel and their managers are responsible for proper collection, use, maintenance, and dissemination of PII residing on individually assigned network and local storage space. All USAID personnel are responsible for compliance with the USAID privacy policies and procedure s, and related records retention and information security procedures. This PIA covers both CONUS and Mission AIDNet systems.

DMZ: The USAID Demilitarized Zone (DMZ) is a physical or logical sub-network that contains and exposes USAID's external services to the public internet or other outside un-trusted network. The DMZ is the buffer area between USAID systems and outside systems. This PIA covers Mission, ALLNet, and Web Services DMZ systems. Any Pll housed on the DMZ must have been cleared for public access before being posted to a system on the DMZ. System owners and program managers are responsible for the proper dissemination of PII in specific systems that use the DMZ.

2.1.2 Describe the SYSTEM and its PURPOSE.

WIRELESS: The USAID Wireless solution encompasses five components: the Array (i.e. an "intelligent" access point), a power injector (to support Power over Ethernet capabilities), the Wireless Management System, and the end user devices, which require a wireless Network Interface Card. The system will provide authentication of wireless USAID sanctioned Guest Users needing access to the Internet and wireless USAID AIDNet account holders.

ALLNet: The USAID Alliance Network (ALLNet) is a robust data network designed to facilitate the communication and interaction with individuals and groups outside of the USAID network around the world. ALLNet provides a forum for the creation of applications to facilitate communication and knowledge sharing between USAID, its partner organizations, and Foreign Service Nationals (FSNs). ALLNet provides USAID with an extranet LAN and is a platform for the hosting of applications that can be securely shared between USAID personnel and other groups they designate. It allows USAID to improve the efficiency of project implementation by providing tools and resources directly to the partner organizations implementing the projects.

AllNet provides worldwide communications between USAID headquarters, field offices in remote locations, other Federal agencies, and implementing partners. ALLNet processes sensitive but unclassified (SBU) information, specifically information and technology management and humanitarian aid information in support of USAID's mission. System owners and program managers are responsible for the proper collection, use, maintenance, and dissemination of PII in specific systems that use ALLNet infrastructure. The systems using ALLNet infrastructure that collect, use, maintain, or disseminate PII are covered by their own separate Privacy Impact Assessments (PIAs). The infrastructure for these systems is covered in this PIA, which includes PII protection during transfer within USAID and between USAID and outside systems, and PII protection at rest in shared and local storage. PII protection during use by a USAID system is covered by the individual PIA for the specific system.

DEVNet: The USAID Development Network (DEVNet) is a logically separated network environment where development, testing, evaluation s, proof-of concepts, and other similar activities can take place without placing AIDNet at risk., primarily located primarily at Terremark in Miami, FL, and Washington, DC, for designated users from USAID Washington . Data is used for the purposes of systems testing and research. N This PIA covers the Pre-Production Lab within DEVNet.

2.1.3 What is the SYSTEM STATUS?

☐ New System Development or Procurement

☐ Pilot Project for New System acquisition 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:

☐ 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
☒ 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

☐ Biometric Data or Related Data

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

☒ 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: IT Operations Division (M/CIO/ITO)

☐ 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 U.S.C. 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?

AIDNet, ALLNet, DEVNet, DMZ, and Wireless do not use PII, but provide the infrastructure for other systems that are responsible for the PII. Some systems that use AIDNet infrastructure collect, use, maintain, and disseminate PII in order to support the Agency's capability to ALLNet infrastructure to provide foreign assistance in over 100 countries. The systems using AIDNet and that collect, use, maintain, or disseminate PII are covered by their own separate PIAs. USAID staff members use the information to promote broadly shared economic prosperity; strengthen democracy and good governance; improve global health, food security, environmental sustainability and education; help societies prevent and recover from conflicts; and provide humanitarian assistance in the wake of natural and man- made disasters.

Various systems collect, use, maintain, or disseminate PII using the AIDNet and ALLNet infrastructures and environment; these systems are covered by their own separate PIAs. ALLNet also uses PII to provide access management services for the collaboration services. DEVNet does not use PII, because the systems that are being developed in this environment do not have the authorization to use SBU without an Authority to Operate. Various systems collect, use, maintain, or disseminate PII using the Wireless transit and the DMZ protection infrastructure and environment; these systems are covered by their own separate PIAs.

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

AIDNet, ALLNet, DMZ, and Wireless do not use PII. DEVNet uses data for testing and research purposes, but is not authorized to use PII. The system owners and program managers of systems that use AIDNet infrastructure are responsible for the proper collection of PII by specific systems that use this infrastructure. The systems using this infrastructure that collect, use, maintain, or disseminate PII 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:

AIDNet, ALLNet, DEVNet, DMZ, and Wireless do not use data collection forms or surveys. Some systems that use AIDNet infrastructure use data collection forms or surveys. The system owners and program managers of systems that use AIDNet infrastructure are responsible for any data collection forms or surveys. The systems using this infrastructure that collect PII via forms or surveys 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: IT Operations Division (M/CIO/ITO), Office of the Chief Information Officer, Bureau for Management

☐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?

AIDNet, ALLNet, DMZ, and Wireless do not collect PII. DEVNet uses data for testing and research purposes, but is not authorized to collect or use PII. The system owners and program managers are responsible for the proper collection of PII by specific systems that use AIDNet and ALLNet infrastructure. The systems using AIDNet and ALLNet infrastructure that collect, use, maintain, or disseminate PII 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?

AIDNet, ALLNet, DMZ, and Wireless do not use PII, but provide the infrastructure for other systems that are responsible for the PII. DEVNet uses data for testing and research purposes, but is not authorized to use PII. The system owners and program managers are responsible for the PII quality and integrity of specific systems that use AIDNet and ALLNet infrastructure. The systems using AIDNet and ALLNet infrastructure that collect, use, maintain, or disseminate PII are covered by their own separate PIAs.

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

AIDNet, ALLNet, DMZ, and Wireless do not use PII, but provide the infrastructure for other systems that are responsible for the PII. DEVNet uses data for testing and research purposes, but is not authorized to use PII. The system owners and program managers are responsible for the PII quality and integrity of specific systems that use AIDNet and ALLNet infrastructure. The systems using AIDNet and ALLNet infrastrncture that collect, use, maintain, or disseminate PII are covered by their own separate PIAs.

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?

Not applicable. These system do not use PII directly.

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.

3.4.6 Does the system monitor or track individuals?

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

☐ No:

☒ Yes: AIDNet and ALLNet monitor and track users to provide access management and control for USAID systems. DEVNet, DMZ, and Wireless do not monitor or track individuals.

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?

System owners and program managers are responsible for the proper collection, use, maintenance, and dissemination of PII in specific systems that use AIDNet and ALLNet infrastructure. The systems using AIDNet and ALLNet infrastructures that collect, use, maintain, or disseminate PIT are covered by their own separate Privacy Impact Assessments (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?

System owners and program managers are responsible for the proper collection, use, maintenance, and dissemination of PII in specific systems that use AIDNet and ALLNet infrastructure. The systems using AIDNet and ALLNet infrastructures that collect, use, maintain, or disseminate PII are covered by their own separate Privacy Impact Assessments (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?

System owners and program managers of cloud computing services that are accessed through the AIDNet and ALLNet infrastructures are responsible for the proper protection of and access to PII collected, used, maintained, and disseminated. The systems using AIDNet and ALLNet infrastructures that collect, use, maintain, or disseminate PII are covered by their own separate Privacy Impact Assessments (PIAs).

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?

Not applicable. System does not collect PII from individuals directly.

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

☒ No

☐ 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?

System owners and program managers of cloud computing services that are accessed through the AIDNet and ALLNet infrastructures are responsible for the proper notification of individual whose PII is collected, used, maintained, and disseminated. The systems using AIDNet and ALLNet infrastructures that collect, use, maintain, or disseminate PII are covered by their own separate Privacy Impact Assessments (PIAs).

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

System owners and program managers are responsible for the proper collection, use, maintenance, and dissemination of PII in specific systems that use AIDNet, ALLNet, DEVNet, DMZ, and Wireless infrastructure. The systems using this infrastructure that collect, use, maintain, or disseminate PII are covered by their own separate PIAs, and so the PII protection during use by a USAID system is covered by the individual PIA for the specific system.

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?

AIDNet, ALLNet, DEVNet, DMZ, and Wireless do not control the s haring of PII outside of USAID. System owners and program managers are responsible for the proper collection, use, maintenance, and dissemination of PII in specific systems that use AIDNet and ALLNet infrastructures. The systems using AIDNet and ALLNet infrastructures that collect, use, maintain, or disseminate PII 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.

☐ 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?

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)

☐ 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