WebPASS Post Personnel System (PS) Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
WebPASS Post Personnel System (PS)
Approved Date: November 3, 2015

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.

In support of the Chief of Mission's responsibility for draw down and evacuation during crises, data for overseas employees and the Washington Bureaus and Offices is automatically transferred from the Centralized to the Global database on a nightly basis. The Centralized database is used to store data maintained by the webPASS users and the Global database is data repository not accessible by the webPASS users. Direct hire and FSN data is then sent to Department of State (DoS) HR/EX, who consolidates all Mission personnel information and sends it back to the Embassy. Data related to the Washington Bureaus and Offices is not transferred to DoS HR/EX.

Used by Washington to report on staffing for Direct Hires and PSCs. This includes the names, SSNs, locations, positions and other HR information as designated by the individual USAID organization.

2.1.2 Describe the SYSTEM and its PURPOSE.

In support of the Chief of Mission's responsibility for draw down and evacuation during crises, data for overseas employees and the Washington Bureaus and Offices is automatically transferred from the Centralized to the Global database on a nightly basis. The Centralized database is used to store data maintained by the webPASS users and the Global database is data repository not accessible by the webPASS users. Direct hire and FSN data is then sent to DoS HR/EX, who consolidates all Mission personnel information and sends it back to the Embassy. Data related to the Washington Bureaus and Offices is not transferred to DoS HR/EX.

Used by Washington to report on staffing for Direct Hires and PSCs. This includes the names, SSNs, locations, positions and other HR information as designated by the individual USAID organization.

Missions use portions of the personnel system, including salary/budget, space, awards, languages, training and dependents. WebPASS is a moderate risk system.

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:

2.1.3 What is the SYSTEM STATUS?

☐ 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

☐ Web Site or Application Used for Collaboration with the Public

☐ Advertising Platform

☐ Website or Webserver

☒ Web Application

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

- ☐ 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 – For FSNs

☐ 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: USAID/HCTM/PPSM - Owns Mission Direct Hire and FSN information as well as the Washington Bureau and Office information.

☒ Another Federal Agency: DoS HR/EX - system of record for Mission FSN information

☐ 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?

USAID PIT information is transmitted to DoS HR/EX as per PII MOU signed on August 24, 2006. An updated version of this document is being worked on currently.

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

In support of the Chief of Mission’s responsibility for draw down and evacuation during crises, data for overseas employees (FSNs and PSCs) is entered into a Centralized database. Mission Data is then sent to DoS HR/EX, who consolidates all Mission personnel information and sends it back to the Embassy.

Used by Washington to report on staffing for Direct Hires and PSCs.

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

WebPass PS is a GOTS system provided by the Department of State. USAID does not add fields to the system but decides which fields provided by DoS it will use. Fields have not been changed in four years.

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: USAID Office: USAID/HCTM/PPSM - Owns Mission Direct Hire and FSN information as well as the Washington Bureau and Office information.
☒ Another Federal Agency: DoS HR/EX - system of record for Mission FSN information
☐ 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?

PII is entered by HR staff in the Mission. It is not entered by the individual themselves.

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?

HR mandated that data should be kept up-to-date. On a bi-annual basis, HR requires that each organization within USAID attest to the validity of its data.

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

Pll is validated by the Mission HR representatives. HCTM also reviews the data and send reports on an ongoing basis to Missions whose data does not fit the necessary criteria (invalid values, missing data, etc.). Mission HR representatives can make updates as necessary.

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 program is defined and driven by the Department of State. USAID follows the process as defined by DoS.

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?

There are several reports for the system. There are some that provide the people, positions and salaries and number of desks available at the mission.

3.4.6 Does the system monitor or track individuals?

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

☐ No.

☒ Yes: System has audit logs that track when users log into the system.

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?

Data collection is done by the mission HR Staff. Not sure of the consent process

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?

PII is entered by HR staff in the Missions. It is not entered by the individual themselves.

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 cloud computing. All data contained within AIDNet.

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: Name

3.7.2 How do you provide notice to individuals regarding?

1) The authority to collect PII: The Foreign Assistance Act of 1961, as amended.

2) The principal purposes for which the PII will be used: Human Capital and Talent Management and the Missions use WebPASS to enable the Missions to have a personnel system, as well as allowing for non-Direct Hire reporting.

3) The routine uses of the PII: Human Capital and Talent Management and the Missions use WebPASS to enable the Missions to have a personnel system, non- Direct Hire reporting, and to support personnel evacuations.

4) The effects on the individual, if any, of not providing all or any part of the PII: No opportunity to consent is provided to users, as the information is collected for personnel in-processing at each Mission.

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

☐ No

☒ Yes: STATE-25, Overseas 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?

N/A

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

HCTM, Organizational and CIO Administrators and the Mission HR staff.

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?

Data is sent to Department of State HR/EX who provides the information back to the Embassies.

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: Department of State

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?

WebPASS data is not provided to public entities.

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