Cross Match Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
Cross Match
Approved Date: June 18, 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.

The Office of Security (SEC) provides security services to protect USAID personnel and facilities, safeguarding national security information, and promoting and preserving personal integrity. SEC receives investigative authority from the Director of National Intelligence and the Office of Personnel Management to conduct personnel security investigations for USAID and all other Federal Agencies/Departments permitted under the delegation.

2.1.2 Describe the SYSTEM and its PURPOSE.

SEC gathers information in order to create investigative records, which are used for processing personal security background investigations to determine eligibility to be awarded a federal security clearance, suitability or fitness determination for federal employment, access to federally owned/controlled facilities and access to federally owned/controlled information systems. In conducting background investigations, the categories of records maintained in SEC's case management system include: name; address; date of birth; social security number (or other identifying number); citizenship status; information regarding an individual's character, conduct and behavior in the community where they presently live and/or previously lived; arrests and/or convictions; medical records; educational institutions attended; employment records; reports from interviews and other inquiries; electronic communication cables; facility access authorizations/restrictions; photographs, fingerprints; financial records including credit reports; previous clearances levels granted; resulting clearance levels; documentation of release of security files; request for special access; records of infractions; and records of facility accesses and credentials issued. The fingerprints are used to confirm a subject's identity through individualization and reveal if a subject has any criminal history for future determination of employment and character suitability.

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

2.1.3 What is the SYSTEM STATUS?

☐ 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

☐ Third-Party Website or Application

2.1.6 What type of system and/or TECHNOLOGY is involved?
☐ 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: (SS-87)
☐ 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:
☐ 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?

1. Privacy Act of 1974, (5 U.S.C. 552a)
2. Executive Order 10450: Security requirements for Government Employment
3. Homeland Security Presidential Directive 12 (HSPD–12): Policy for a Common Identification Standard for Federal Employees and Contractors
4. Executive Order 12968: Access to Classified Information
5. Executive Order 12333: United States Intelligence Activities
6. Executive Order 13381: Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information;
7. Executive Order 13467: Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information
8. Executive Order 13488: Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust and the Intelligence Reform and Terrorism Prevention

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

1. The Office of Security gathers PII in order to create investigative records, which are used for processing personnel security background investigations to determine eligibility to be awarded a federal security clearance, suitability or fitness determination for federal employment, access to federally owned/controlled facilities and access to federally owned/ controlled information systems.
2. The categories of PII used are name, address, date of birth, social security number (or other identifying number), and citizenship status. The Office of Security needs this specific PII to assess an individual's character for obtaining a federal security clearance, suitability or fitness determination, access to federally owned/controlled facilities and/or information systems. Without these PII elements, The Office of Security would not be able to operate as we would not be able to obtain the following: conduct and behavior in the community where the applicant/employee presently lives and/or previously lived, arrests and/or convictions, medical records, educational institutions attended, employment records, reports from interviews and other inquiries electronic communication cables, facility access authorizations/ restrictions, photographs, fingerprints, financial records including credit reports, previous clearances levels granted, resulting clearance levels, documentation of release of security files, request for special access, records of infractions, and records of facility accesses and credentials issued.
3. FIPS 201-1 Guidance on Required Background Checks Prior to PIV Card Approval/Issuance.
4. Before issuing the PIV Card, the process shall ensure that a previously completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation is on record. In the absence of a record, the required federal background investigation shall be initiated.(10) The PIV Card should not be issued before the results of the NAC are complete. However, if the results of the NAC have not been received in 5 days, the PIV Card may be issued based on the FBI NCHC. In the absence of an FBI NCHC (e.g., due to unclassifiable fingerprints) the NAC results are required prior to issuing a PIV Card. The PIV Card shall be terminated if the results of the background investigation so justify

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

NA

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 (SS-87)
- ☐ 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:

☐ 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?

Data is collected on site and in person for all data collected.

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?

The system operator reviews data to insure the individual ID's reflects its process.

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

Each person must show a State ID validating the information on site. The information is deleted after 30 days.

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 minimum PII relevant and necessary to accomplish the legal purpose of the program are name, address, date of birth, place of birth, social security number (or other identifying number), and citizenship/legal status.

1. The categories of PII used are name, address, date of birth, social security number (or other identifying number), and citizenship status. The Office of Security needs this specific PII to assess an individual's character for obtaining a federal security clearance, suitability or fitness determination, access to federally owned/controlled facilities and/or information systems. Without these PII elements, The Office of Security would not be able to operate as we would not be able to obtain the following: conduct and behavior in the community where the applicant/employee presently lives and/or previously lived, arrests and/or convictions, medical records, educational institutions attended, employment records, reports from interviews and other inquiries electronic communication cables, facility access authorizations/ restrictions, photographs, fingerprints, financial records including credit reports, previous clearances levels granted, resulting clearance levels, documentation of release of security files, request for special access, records of infractions, and records of facility accesses and credentials issued.

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?

NA

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?

The PII is mandatory to SEC receives investigative authority from the Director of National Intelligence and the Office of Personnel Management to conduct personnel security investigations for USAID and all other Federal Agencies/Departments permitted under the delegation. If someone refuses to take a fingerprint... well that doesn't happen. We would have two options (1) Cancel the investigation due to non-compliance and/or an inability to receive full coverage to conduct the investigation without the cards or
(2) Substitute the cards with local agency checks and NCIC checks.

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?

If PII is incorrect on the hardcopy FP, SEC will send the document back to the requester/selecting official as a rejection sighting the errors and corrections to be made. The hardcopy FP card will then need to be resubmitted via the requester. Electronic FP cards typically don't have incorrect information and if they do, then SEC has to work with the agency who receives the prints, OPM, to get the errors corrected. This is typically done via phone call from SEC to OPM's office.

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?

NA

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: The person is notified that the information being provided is to be used to conduct a security investigation background based on their employment with the Federal Government.

2) The principal purposes for which the PII will be used: To complete a fingerprint check with the FBI for suitability for employment.

3) The routine uses of the PII: A part of the investigative file to complete their investigation.

4) The effects on the individual, if any, of not providing all or any part of the PII: A complete security investigation will not be able to be completed thus impacting their ability to be employed by the Federal Government.

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

☐ No

☒ Yes: AGENCY FOR INTERNATIONAL DEVELOPMENT Privacy Act of 1974, System of Records, march 15, 2013, USAID 008

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?

NA

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

Office of Security personnel in the Investigation Division and Domestic Security Branch. The PII that is accessible is the name, DOB and SSN. The Investigation Division receives the information in hard copy. The Domestic Security Branch receives the information from the applicant. The users only receive the information if that particular case is assigned to the employee.

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?

The Office of Security (SEC) provides security services to protect USAID personnel and facilities, safeguarding national security information, and promoting and preserving personal integrity. SEC receives investigative authority from the Director of National Intelligence and the Office of Personnel Management to conduct personnel security investigations for USAID and all other Federal Agencies/Departments permitted under the delegation. Information collected is for investigative purposes collected by OPM. No engagement with the public.

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: Only if you consider transmitting this information to OPM for its intended purposes. It is transmitted in the same manner as SIDS system.

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?

No PII from this process can be provided to USAID or service providers.

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