Security Investigative Database (SID) Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
Office of Security / Security Investigative Database (SID)
Approved Date: May 24, 2017

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: The Agency partners with others to end extreme poverty and promote resilient, democratic societies while advancing our security and prosperity.

The Office of Security, Personnel Security Division (SEC/PS), manages the personnel suitability and security clearance program. When an applicant, employee or contractor requires facility access or access to classified national security information, that individual must be granted facility access or a security clearance at the proper level to access that information. Logical access is also provided based on clearance of the individual by SEC investigators. SEC reviews and analyzes investigations of employment candidates, employees and others seeking access to USAID to ensure that granting an individual facility access and/or access to classified information is consistent with the interests of national security.

The three security clearance levels are Confidential, Secret and Top Secret. The purpose of a security clearance is to determine whether an applicant or employee is able and willing to safeguard classified national security information or perform sensitive duties, based on their loyalty, character, trustworthiness and reliability.

SEC conducts and adjudicates background investigations of applicants, employees and others seeking access to USAID and ensures that granting an individual that access is clearly consistent with the interests of national security.

2.1.2 Describe the SYSTEM and its PURPOSE.

The USAID Office of Security (SEC) uses the Security Investigation Database (SID) application to create database records that track and store personal background information during the investigative process for all Agency employees. This Commercial-of-the-Shelf (COTS) system will improve quality of service, reduce process time and be capable of supporting future mandatory requirements and mandates as defined by Office Director of National Intelligence (ODNI). SID a moderate risk level major application.

SEC requires the system to communicate with office of Human Capital and Talent Management (HCTM), Office of Personnel Management (OPM), and the Federal Bureau of Investigation (FBI) offices. *(The interconnection of the databases is more of a transfer than a one-to-one connection, and the transfer of the data is done via flat files that are transported via services or batch jobs to and from the SID system. Services are connected as outlined in the SSP system diagram via a secure method either SSL, VPN, etc. The batch jobs are local jobs that run on the application server and are for the most part data imports. The server is hardened using USAID standard build documentation.)* SID completely automates the tracking and storing of the background personnel investigations process by allowing connectivity were ever it is possible to other databases (OPM and FBI) that support the conduct of a background checks. SID will connect electronically with other like systems in other agencies or departments of the U.S. Government, such as with Office of Personnel Management (OPM) and their e-QIP system, which allows government and contractor employees to complete a personnel background questionnaire electronically any were in the world and send it back to OPM securely. The SID system does connect to OPM and transfer the completed questionnaire in SID and automatically populate the database.

The SID system receives and transmits data to the FBI for finger print and name check. This is done via the MOU that is in place with the FBI. The data is transmitted via scripts that run on the JBOS server and are automatically updated into the SID database. The SID system also has an additional connection to OPM. This connection is facilitated thru a mail server running on the production environment. This is how data is transported from OPM into SID. An example of this data would be the applicant's e-QIP form.

SID database has transparent data encryption (a.k.a. "data at rest" encryption) and uses AES256 (256-bit) standard/algorithm for encryption. SID has its own dedicated database which is housed in a separate Oracle home on the database server and is logically segregated from other database instances/environments running on the same server.

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 - Items that are present in the system are either scanned into SID, manually entered by the investigator assigned the case, or are imported via an automated mechanism.

Record Management (Hard Copies): Investigators are instructed to not save any PII onto their personal computers. Any PII that is scanned or created on an investigator's laptop is removed from the investigator's laptop once uploaded to SID. PII removal is performed by the investigator. There is no verification in place that it was done. Hard copies are to be destroyed via the NARA Schedule 18.

Retention Periods: SID follows ADS Chapter 502 "Records Management Program" for the maintenance, archival, and disposal of records. Section 502.3.6 of this document outlines the standards followed for record schedules. SID data falls under NARA Schedule 18.

2.1.5 Does your program participate in PUBLIC ENGAGEMENT?

☒ No. The only part of the public that provides information to the SID system is individuals with information on proposed and/or current USAID employees, contractors, and vendors.

☐ 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.) AIDNet

☒ Network

☒ Database

☒ Software

☒ Hardware: Virtual Linux and Oracle servers located in USAID Data Center

☐ 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. This is hosted on AIDNet and is not public facing.
☐ 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: Spouses of USAID applicants and employees/PSCs, as appropriate to meet the Federal Investigative Standards
☐ 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 (The only access to SID in production is SSO. There are no usernames and passwords used by SID.)
☐ Unique Device Identifier (Device information is not store in SID. Items such as IP address are stored in the Audit Logs only but do not reside in the actual SID system.)
☐ Location or GPS Data
☐ Camera Controls (photo, video, videoconference)
☐ Microphone Controls
☐ Other Hardware or Software Controls
☐ Photo Data (The only photos that may be present may be part of a scanned copy of a driver's license or passport.)
☐ 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)

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☐ 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: Kelly McClellan, Office of Security, USAID SID System Owner. Office: SEC/PSD
☐ 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?
Executive Order 10450: Security requirements for Government Employment. **Homeland Security Presidential Directive 12 (HSPD–12):** Policy for a Common Identification Standard for Federal Employees and Contractors. **Executive Order 12968:** Access to Classified Information. **Executive Order 13488:** Granting receptivity on federal service and federal contractor employee fitness and reinvestigating individuals in positions of public trust. **Executive Order 12333:** United States Intelligence Activities.

3.1.1 What are the statutes or other LEGAL AUTHORITIES that permit you to collect, use, maintain, or disseminate personal information?

Executive Order 13381: Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information.
Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458).
Federal Investigative Standard

Memoranda of Understandings that are In Place:
(Please see the MOUs loaded into CSAM)

1.) **OPM**
2.) **FBI**

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

The PII is collected 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 determination for federal employment, access to federally owned/controlled facilities and access to federally owned/controlled information systems.

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

Potential new uses for the information would be brought to the attention of the Director of Management Policy Budget and Performance (M/MPBP) to evaluate the merit of the new use. If the use was considered worthwhile, the Director of M/MPBP would consult with the USAID General Counsel and the USAID Privacy Office to evaluate legal and privacy concerns of the new use.

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)

- AID 6-85: Foreign Activity Data
- AID 500-6: Dual Citizenship Questionnaire
- Drug Use Questionnaire and Statement to Remain Drug Free
- OMB 0412-0549: Education Lead
- OMB 0412-0549: Employment Lead-Company
- OMB 0412-0549: Employment Lead-Supervisor
- IG Lead (SID Internal Forms)
- IG-I Spouse (SID Internal Forms)
- INS Inquiry (SID Internal Forms)
- INS Spouse Inquiry (SID Internal Forms)
- INS Other Inquiry (SID Internal Forms)
- Foreign National Contact Form (required by CIA for SCI access)

3.2.1 Do you use any data collection forms or surveys?

- OMB 0412-0549: LAC General Inquiry
- F-APD-0044: LAC Alexandria, VA Police Department Inquiry
- PD 70: LAC DC Metropolitan Police Department Inquiry
- OMB 0412-0549: LAC NYC Police Department Inquiry
- Medical and Mental Health Questionnaire (SID Internal Forms)
- Military Records Inquiry
- OFI Form 86C: NCIC Inquiry (OPM Form)
- OFI Form 86C: NCIC Spouse Inquiry (OPM Form)
- OS Request Letter (SID Internal Forms)
- Passport Request (SID Internal Forms)
- OMB 0412-0549: Personal Reference
- OMB 0412-0549: Residence Lead
- FinCEN Form 50: FinCEN Check
- SF85, SF85P, SF86 (from OPM/eQIP)

☐ 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: Kelly McClellan, Office of Security, USAID SID System Owner. Office: SEC/PSD
☐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?

The PII placed on SID is obtained from eQIP/eDelivery from OPM, internal USAID background investigations case management system or from the subject or subject's references. Everything placed on SID for investigators comes from a secure and trusted source, either from the confines of the USAID network or from the eQIP system.

Data is also collected directly from the subject as well as from authoritative sources, which include police records, credit records, public records, current and previous employer records and subject-provided personal references. All of the paper documents are scanned into SID as an electronic copy and then the paper copy is destroyed. Subjects who undergo background investigations have the opportunity to review the results of the investigation to ensure that no data (not provided by the subject) is incorrect.

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?

Data is also collected directly from the subject as well as from authoritative sources, which include police records, credit records, public records, current and previous employer records and subject-provided personal references. Subjects who undergo background investigations have the opportunity to review the results of the investigation to ensure that no data (not provided by the subject) is incorrect.

Furthermore, Adjudicators review and adjudicate all information presented as a statement/evidence as a whole against all the information received on a subject. The Adjudicators look for discrepancies, which are noted in the decision report.

Individuals requesting amendment of their record(s) maintained by USAID must follow the "Contesting Record and Record Access Procedures" outlined in SORN USAID-008.

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

Individuals requesting amendment of their record(s) maintained by USAID must identify the information to be changed and the corrective action sought. Requests must follow the "Contesting Record and Record Access Procedures" outlined in SORN USAID-008. Additionally, PII is automatically updated in the system when an eQIP form is imported. Also, if someone has a name change, etc. that documentation is uploaded in the subject's record and the change is made by an internal SEC employee (such as a Case Controller).

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?

A wide array of PII is collected so that a thorough background investigation of an individual can be performed. Initial identifier information is required to ensure that the individual is who they claim to be. Additionally, extensive background information is needed to ensure that the individual does not pose a threat to the security of the United States Government in the position/role for which they are being considered. To obtain a level of assurance that is adequate, investigations should include employment history, credit history, criminal history, education history, medical history, and relationships with foreign countries and foreign nationals. All application information is filed and sorted by name and SSN. SSNs are required to query and retrieve all information in the SID system.

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?

Users can create two distinct reports:

1.) Report of Investigation: This report contains all of the information that is present in the investigation package. The report can be generated by the Field Investigation Group.
   a. PII Included:
      i. Cover Page: Subject's name, DOB, POB, SSN.
      ii. Report: Names, addresses and contact information of references and all results and reported information.
2.) Adjudication Summary with Decision Report: This report contains summary information about the subject of the investigation along with Adjudicator notes and the outcome of the report.
   a. PII Included:
      i. Cover Page: Subject's name and case number
      ii. Report: Adjudicative guidelines present in the case, case facts related and mitigating information.

3.4.6 Does the system monitor or track individuals?

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

☐ No.

☒ Yes: Log data kept about how long users are accessing the SID system and if there was a successful or failed log in attempt. Audit trail reports are present and can be accessed by the SID system administrator. The Audit Trail reports allow administrators to determine what a specific user accessed, updated, changed, and imported. The logs also track what investigations an investigator views.

There are also automated processes in place to alert administrators if one of the two conditions occur:

3.4.6 Does the system monitor or track individuals?

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

1.) A user attempts to access a "restricted" investigation which will result in an automated email follow up report being created.
2.) A user attempts to access his/her own investigation which will result in an automated email and follow up report being created.

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 provision of PII is voluntarily but essential to carrying out the investigatory process and that the subject must consent to certain collections to move forward with the process, such as providing written consent to perform credit checks, FBI name check, and other. The PII collection and consent is mandatory to perform the security background investigation and subjects who do not consent are not eligible for employment. Information is collected from individuals through eQIP, government-created general service forms, and USAID forms, all of which have a consent clause for the individual to explicitly allow or deny (by not signing) consent for PII collection and sharing.

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 only ways a subject may access information maintained in the system is by submitting a FOIA/Privacy Act Request or by following the "Contesting Record and Record Access Procedures" outlined in SORN USAID-008.

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?

Not applicable. SID does not use cloud computing.

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, SSN, and Employee ID Number are saved as the primary keys.

3.7.2 How do you provide notice to individuals regarding?

N/A. SID does not include a privacy policy or notice due to the fact that individuals who have data maintained in the system do not have access to the system.

Notices that are given to the individuals that are undergoing a background check are extensive and the notices state what the PII collected will be used for. The individual subjects must sign off on the following releases:

- AID 500-3: Security Investigation and Clearance Record
- AID 500-4: Fair Credit Reporting Act of 1970, As Amended
- AID 500-5: Notice Required by the Privacy Act of 1974
- AID 500-11: Medical and Mental Health Authorization
- IRS 4506-T
- Tax Information Authorization Form 8821
- Certification of Release (included with SF form from eQIP-not USAID specific)
- Release of Information (included with SF form from eQIP-not USAID specific)
- Medical Information Release (included with SF form from eQIP-not USAID specific)

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

☐ No

☒ Yes: USAID SORN-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?

N/A. SID does not involve cloud computing.

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

Investigators and Adjudicators who are assigned to the investigation by the Program Manager and system administrators will have access to PII when their need-to-know has been verified.

Role assignment provided by the Program Manager will determine who has access to what investigation and what level of access each user will have.

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?

PII is shared outside of USAID upon request and the requestor information is recorded and stored in SID. Below are the two methods for PII sharing, both are completed via USAID approved methods either via OPM's NP2 Portal, or via delivery receipt hard copy mailing.

1.) Routine uses of the applicable SORN.

2.) Other Federal, State, Military, and Local Government Agencies for reciprocity purposes.

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: Outside request made to SEC:
Request sent to SECClearanceVerif@usaid.gov with encrypted method for PII transmittal
If person is located in OPM's NP2 portal, SEC will send file/information using that method
If OPM's NP2 is not an option, SEC will send encrypted information using SECClearanceVerif@usaid.gov

SEC requests information from outside agency:
SEC will send PII encrypted if OPM's NP2 option is not available. (OPM, DOS, and majority of DHS file requests are available through OPM's NP2.) SEC will request that information is sent through OPM's NP2 or encrypted back to SECClearanceVerif@usaid.gov.

Note: The majority of files and case information are sent through the OPM's NP2 portal. If the recipient does not have a portal account, the requesting agency will normally send an Agent in person to pick up the requested file. In rare cases USAID/SEC will send the file via email after encrypting it.

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.

There are two methods for which PII enters the system:

1.) The applicant can make PII available to USAID through explicit consent or providing the PII himself or herself.

2.) An automated import from either OPM or the FBI can make PII available. However, this is only if the applicant has given consent for the background investigation to take place.

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