C-CURE Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
Approved Date: July 15, 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 Office of Security (SEC) provides centralized security support to the Agency and ensures that appropriate liaison with the Department of State's Bureau of Intelligence, Bureau of Research, and Bureau of Diplomatic Security is conducted on a daily basis. The Domestic Security Branch (SEC/ISP/DS) operates and controls the physical security programs for the USAID headquarters building and other USAID facilities in the Washington, DC Metropolitan area.

2.1.2 Describe the SYSTEM and its PURPOSE.

SEC/ISP/DS utilizes the Computer Coordinated Universal Retrieval Entry (C-CURE) system to manage certain aspects of the automated facility access control system, including: Badge Management, automatic replication, revocation of badges, and automated access control for USAID workspaces within Ronald Reagan Building, SA-44, SA-41, and the USAID COOP Site.

The information in C-CURE is collected from potential USAID employees and contractors during the employment process, and is mandatory for employment -- refusal to provide this information impacts hiring of the individual. Collection of this information is captured on an application form, AID Form 500-1, Request for Federal Identification Card/Facility Access Card, by the requester through their Bureau/Independent Office Administrative Officer.

Categories of records maintained in the system are: card/number, personnel clearance, employment status of present USAID employees and contractors, and individual photo. SEC gathers this information so the individual employees of USAID can be verified that they are who they say they are when requesting assess to USAID office space or upon request of other USAID employees.

C-CURE runs on a closed Windows network in the Ronald Reagan Building over a dedicated fiber connection. C-CURE has no interconnections and remote access to the system is not permitted. C-CURE is backed up at two locations (SA-44 and the Agency COOP site) where the system can be accessed and operated, in the event that the primary server becomes inoperable.

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

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

2.1.6 What type of system and/or TECHNOLOGY is involved?
☐ 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
☐ Bring Your Own Device (BYOD)
☐ Remote, Shared Data Storage and Processing (cloud computing services)
☒ Other: COTS software C-CURE 9000 from Software House
☐ 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
☒ Security Clearance
☒ Biometric Record (signature, fingerprint, photo, voice print, physical movement, DNA marker, retinal scan, etc.)
☒ Sex or Gender

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☐ Age
☐ Other Physical Characteristic (eye color, hair color, height, tattoo)
☐ Sexual Orientation
☐ Marital status or Family Information
☐ Race or Ethnicity
☐ Religion
☒ Citizenship
☒ Other: USAID Employment Status and PIV Card Number
☐ 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: PIV card photograph
☐ 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

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☐ 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: Office of Security, Domestic Security Branch
☐ 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?
SEC gets its legal authority for maintaining this system from the following Executive Orders and Public Law: Executive Order 10450: Security Requirements for Government Employment: Homeland Security Presidential Directive 12 (HSPD-12); Policy for Common Identification Standard for Federal Employees and Contractors: Executive Order 113526: Access to Classified Information 12333: United States Intelligence Activities; Executive Order 13381; Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information and the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458).

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

SEC gathers this information to verify the identities of employees and contractors to control access to USAID facilities.

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

SEC will respond to ad hoc requests from the Office of General Counsel for reports, when the data is needed for an investigative purpose.

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: AID 500-1, Request for Federal Identification Card/Facility Access Card
- ☐ 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: Office of Security, Domestic Security Branch

☐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?

PII is collected from the AID Form 500-1 which is completed by the USAID hiring Bureau with direct input from the individual.

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?

PII is provided by the person to whom it pertains. Further, the potential USAID employee is required to present their AID Form 500-1 form to the SEC Badging Office along with two government issued identifications for verification purposes.

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

USAID employees and contractors are required to renew their USAID PIV annually, involving the submission of a new AID Form 500-1, which allows for PII to be updated and verified at least annually.

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 individual's PII collected, that is, Social Security Number, name and security clearance information, is required for the USAID to verify that persons are who they say they are, before granting access to USAID controlled areas. SSNs is the only means of uniquely identify individuals. SEC uses SSN to uniquely identify individuals, and to access the OPM Central Verification System (CVS) for verification of existing security clearances, background investigations, suitability fitness, and Homeland Security Presidential Directive (HSPD) 12 Personal Identity Verification (PIV) credentialing determination.

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?

C-CURE does not disclose information except in response request for information for legal investigations by Office of General Counsel. These reports disclose physical access logs.

3.4.6 Does the system monitor or track individuals?

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

☐ No.

☒ Yes: SEC monitors the access to USAID controlled facilities, to include buildings and doors, by USAID employees and contractors using the C-CURE system. Audit logs of are maintained of individual's access to doors and buildings.

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 information is collected by SEC from potential USAID employees and contractors during the employment process, and is mandatory for employment -- refusal to provide this information impacts hiring of the individual.

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 employees and contractors are required to submit their updated AID Form 500-1 annually, which provides an opportunity to amend their PII stored in C-CURE.

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?

N/A. C-CURE does not use 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: Records are retrievable by last name, social security number, and/or USAID assigned case number or other unique identifier attributed to the individual.

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:

A Privacy Act Statement is provided on Form 500-1.

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

☐ No

☒ Yes: USAID SORN-08, Personnel Security and Suitability Investigatory 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. C-CURE does not involve cloud computing services.

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

Only individuals with a valid C-CURE local user account have access to the C-CURE system. Only SEC employees working as security specialists, contractor guards, and SEC Senior Staff have access to the C-CURE database. The Office of Security may disclose the information to other Federal agencies so that they can use the issued badges to grant physical access to their Federally-owned or controlled facilities.

3.8.1 Who has access to the PII at USAID?

Users of the C-CURE network are assigned an account profile as their duties dictate with privileges ranging from read only privileges (in which users can see names, badge numbers and expiration date of badges but not make a changes) to limited system administrative privileges (in which users can see the same information as read only can also modify select user information and access as needed). Full control of the system is limited only to the system administrator. Upon termination/registration of an individual with access to the C-CURE system, a request is sent to the system administrator requesting the termination of the account.

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?

SEC may disclose the information to other Federal agencies so that they can use the issued badges to grant physical access to their Federally-owned or controlled facilities.

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?

N/A. C-CURE does not engage directly with the public.

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