PRIVACY IMPACT ASSESSMENT

ConsularOne Platform/Infrastructure (CA CPI)

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Date of completion of this PIA: August 2022
(b) Name of system: ConsularOne Platform/Infrastructure
(c) System acronym: CPI
(d) Bureau: CA/CST
(e) iMatrix Asset ID Number: 253146
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

ConsularOne is a major system modernization effort intended to replace outdated legacy applications. ConsularOne has four different business areas to prevent the duplication of hardware and software components utilized by different ConsularOne services including CA ConsularOne Platform/Infrastructure (CPI), CA ConsularOne Applications and Data (CAD), CA ConsularOne Data Infrastructure (CDI), and the CA ConsularOne Central Services (CCS) system.

The purpose of the CA CPI system is to serve as a common technical infrastructure to provide cross-cutting ConsularOne services and information technology capabilities to meet CA business needs. The CA CPI system platform capabilities support CA business applications to administer consular services. This modernized system moves paper-based services online, allowing citizens and non-citizens to request services from Consular Affairs. Using a Service Oriented Architecture (SOA), the system decouples service capabilities to improve performance, scalability, and speed-to-market. The CA CPI system also hosts infrastructure services such as Identity Access Management (IAM) services to provide identification and authentication services and the Siebel application that supports modernized application services such as the CA Electronic Consular Reports of Birth (eCRBA) and the CA Online Passport Renewal (OPR) systems.

The CA CPI system's main function is to transmit information among the other ConsularOne systems.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The following PII is maintained on both U.S. persons and non-U.S. persons:

- Names
- Birthdates
- Places of birth
- Marriage status
- Surnames/aliases
- Citizenship
- Biometrics
- Photographs
- Passport information
- Social Security Number
- Gender
- Age
- Race
- Hair and eye color
- Height
- Phone number(s)
- Personal Addresses
- E-mail address(es)
- Individual medical information
- Individual education information
- Family information
- Financial Account Numbers of Individuals/other financial information
- Other government identification, e.g., marriage license, divorce papers, naturalization certificate, driver's license, etc.
- National ID (non-U.S. persons only)

- Business contact information: Department of State Consular Officers, Notary or other representatives/petitioner information transmitted via CA CPI. PII can include names, posts, company, business email, organization, and phone number. Business contact information is collected for authentication CA applications. The remainder of the PIA will focus on the information maintained on individuals seeking consular services.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 22 U.S.C 2651a (Organization of Department of State)
- 22U.S.C. 211a (Authority to Grant, Issue and Verify Passports)
- 22 U.S.C. 3904 (Functions of Service)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒Yes, provide:

- SORN Name and Number: STATE-05, Overseas Citizens Services Records and Other Overseas Records
- SORN publication date: September 8, 2016

- SORN Name and Number: STATE-26, Passport Records
- SORN publication date: March 24, 2015

- SORN Name and Number: STATE-39, Visa Records
- SORN publication date: November 8, 2021

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

Schedule number: Awaiting assignment by NARA
Disposition Authority Number:

DAA-0059-2020-017-007
Length of time the information is retained in the system:
Temporary, Destroy when 100 years old.
Type of information retained in the system: Records documenting the issuance, amendment, extension, or renewal of passports. Records include, but are not limited to, passport applications with photographs; applications for amendment or extension and related correspondence; passport authorization records; original copies of requests from other government agencies for renewal, modification, or amendment of an existing fee passport (not original issue); documentation of recovered, surrendered, unclaimed or found passport books; reports of birth of American citizens abroad; certificates of witness to marriage; applications for amendment or extension of passport; certificates of loss of nationality; oaths of repatriation; and all other supporting forms, documents and correspondence pertaining to each case.

Schedule number: Awaiting assignment by NARA
Disposition Authority Number: DAA-0059-2020-0017-0016
Length of time the information is retained in the system:
Temporary. Destroy 25 years after issuance.
Type of information retained in the system: Records documenting the issuance of an immigrant or non-immigrant visa. Records include, but are not limited to, the application, personal and biographic data, adjudication data, visa clearance, name check data, case summary, case status, reports, correspondence, notes, and other supporting documentation regarding the visa applicants.

Schedule number: Awaiting assignment by NARA
Disposition Authority Number: DAA-0059-2020-0017-0027
Length of time the information is retained in the system: Cut off when case is closed or abandoned. Destroy 20 years after cutoff or when no longer needed, whichever is later.
Type of information in the system: Records documenting arrests, citizenship issues, death notifications, financial assistance, loss of nationality, lost and stolen passports, property, citizen registrations, welfare, and whereabouts. Records include, but are not limited to, biographic information, information about the case, and the case activity log.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No ☐N/A

- If yes, under what authorization?
26 U.S.C. 6039E (Information Concerning Residence Status)
22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(d) How is the PII collected?

PII is transmitted from the CA source systems listed in paragraph 6(a) except for CA CCS and CDI which shares non-PII data with the CA CPI system. All data are transmitted database to database. The CA CPI system is a shared platform which provides cross-cutting business, IT capabilities, and information to meet CA business needs.

(e) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

(f) What process is used to determine if the PII is accurate?

The PII received via other CA systems is validated for accuracy via the source system processes in which the applicants request the service. For addresses, information is verified for accuracy via the United States Postal Service.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Information is checked for currency via the source system processes where the applicant is requesting the service. Any updates or changes to applicant information are updated in the source system and automatically updated in CA CPI via the CA systems interfaces listed in paragraph 6(a) below.

(h) Does the system use information from commercial sources? Is the information publicly available?

No. The CA CPI system does not use commercial information, and the information is not publicly available.

(i) How was the minimization of PII in the system considered?

The PII listed in 3(d) are the minimum necessary to perform the actions required by this system. Concerns about collecting and maintain PII include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were assessed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function for which it was intended.

5. Use of information

(a) What is/are the intended use(s) for the PII?

The PII in paragraph 3(d) is used by Consular Affairs to process and administer consular services requested by U.S persons and non-U.S. persons, such as visas, passports, and Electronic Consular Reports of Birth Abroad.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the purpose of the CA CPI system is to serve as a shared platform providing cross-cutting business and IT capabilities with a common technical infrastructure leveraged to meet CA business needs to deliver consular services. The PII shared on the CA CPI system supports the implementation of the eCRBA, American Citizen services, visa, and passport programs.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

(d) If the system will use test data, will it include real PII?

☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal: The term "internal sharing" traditionally refers to the sharing of information within the Department of State (Department), but external to the owning organization (referred to as "bureau" at the Department). However, since the various Bureau of Consular Affairs offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in the CA CPI system shares and exchanges information internally with the CA CDI, CA CCS, CA CAD system, the CA Electronic Payment System (EPS), CA OPR, CA eCRBA, CA Enterprise Service Bus (CAESB), and CA Crisis Management System (CACMS).

External: United States Postal Service (USPS)

(b) What information will be shared?

Internal: Information listed in paragraph 3(d) is shared with the CA systems identified in paragraph 6(a) depending on the requirement to provide the specified consular service requested.

External: Names and addresses are shared with the USPS.

(c) What is the purpose for sharing the information?

Internal: CA CPI shares information internally in order to facilitate the electronic transmission of PII across CA systems listed in paragraph 6(a) and provides the associated storage and transmission devices to support administration and delivery of U.S. persons and non-U.S. persons consular services domestically and overseas.

External: PII is shared with the USPS to validate addresses of individuals requesting CA services.

(d) The information to be shared is transmitted or disclosed by what methods?

Internal: Information is shared database to database by Department approved secure transmission methods for the handling and transmission of sensitive but unclassified (SBU) information.

External: N/A

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal: Safeguards in place for internal sharing arrangements include secure transmission methods such as data encryption using Hypertext Transfer Protocol Secure (HTTPS) and secure communications using Transport Layer Security (TLS) and multiple Transmission Control Protocol/Internet Protocol (TCP/IP) layers. These safeguards are approved by in Department of State policies for handling and transmission of sensitive but unclassified (SBU) information. Electronic files are PIV/PIN or password protected and access is controlled by system managers. Audit trails track and monitor usage and access of systems that reside on the Department's secure intranet network, OpenNet.

External: N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

No. The CA CPI system does not collect information from the public. The CA CPI system information is transmitted from the CA source systems identified in paragraph 6(a). When the collection of information by the source system involves potential PII collected on U.S. persons, there is a Privacy Act statement displayed on the form in which the applicant is seeking a consular service, such as a passport.

Non-U.S. person data are subject to the requirements of the Immigration and Nationality Act (INA)222(f) which are stated on the collection site of the source system collecting the PII.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?
☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

The CA CPI system does not collect information from the public, but instead pulls and transmits information from the systems addressed in paragraph 6(a). Consent is acquired via the source systems in which the information is originally obtained when applicants request consular services.

(c) What procedures allow record subjects to gain access to their information?

Individuals requiring access to their information can follow the procedures outlined in the source system where services are being requested or follow record access procedures outlined in SORNs STATE-05, STATE-26, and STATE-39 to request access to their information request.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Individuals must follow processes of the CA source system to request correction of information. Notice to change personal information is provided at the site where applicants apply for the specific services and/or during the adjudication processes. Individuals can also follow the record access procedures in SORNs STATE-05, STATE-26 and STATE-39 regarding points of contact to inquire about their information.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

CA CPI pulls PII from other CA systems, which resides outside the CA CPI system boundary. Notice on how to correct records are provided via the adjudication process of the source system collecting the information from the individual requesting the specific service and housed in the CA CAD system and transmitted to CA CPI. Individuals can also follow procedures in SORNS STATE-05, STATE-26 and STATE-39, which points to necessary procedures record subjects must follow to correct their information.

8. Security Controls

(a) How is all of the information in the system secured?

The CA CPI system is secured within the Department of State intranet where risk factors are mitigated using defense in depth layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information to perform official duties.

Access to applications is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user's supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

Systems are configured according to the State Department Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institutes of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or mitigated.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

CA Internal Users: Access to the CA CPI system is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. System administrators, database administrators and Department of State employees have access to the system and all the information approved for their specific role to aid in processing citizen services, passport, and visa applications and to perform system and database maintenance**.**

U.S. Citizen and noncitizen public users: The external user is authenticated by CA CPI IAM services to access CA CAD application services using the external user's user id/password credentials. Public users do not have access to CA CPI information. Public user access is limited to the authentication services and their information to acquire passwords to access CA CAD applications and services.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Access to the CA CPI system is role-based and restricted according to approved job responsibilities and requires managerial concurrence. Supervisors and local Information System Security Officers (ISSO) determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function, manager's approval, and level of clearance.

(d) How is access to data in the system determined for each role identified above?

In accordance with Department of State policy, the CA CPI system employs the concept of least privilege to users by allowing only authorized access to information systems and information systems resources necessary to accomplish assigned tasks as approved by the manager. All roles have been analyzed to determine the specific data set and corresponding functions that will be required in accordance with the person's job and level of security approved by the supervisor. Accordingly, when a user or service account is added to a particular database role, access is limited to only the data and functions allotted.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

The CA CPI system audit service on its servers captures many logs, access attempts, and all actions exceeding Department requirements. Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information in the CA CPI system. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures
- Logons after-hours or at unusual times
- Failed attempts to execute programs or access files
- Addition, deletion, or modification of user or program access privileges
- Changes in file access restrictions

The purpose of the audit trail is to document unintended modification or unauthorized access to the system.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

The CA CPI system Security Plan includes information and procedures regarding access to its data.

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All system administrators must take the IA210 System Administrator Cybersecurity Foundations Course which has a privacy component. In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially. The State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy, and integrity.