

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) **Name of system:** ConsularOne Platform/Infrastructure
- (b) **Bureau:** Consular Affairs (CA)
- (c) **System acronym:** CA CPI
- (d) **iMatrix Asset ID Number:** 177406
- (e) Reason for performing PIA:
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable):

3. General Information

- (a) **Does the system have a completed and submitted Security Categorization Form (SCF)?**
 - Yes
 - No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

- (b) **What is the security Assessment and Authorization (A&A) status of the system?**

The initial Assessment and Authorization process is underway and Consular One is expected to receive an Authorization-To-Operate in the Summer 2018.

- (c) **Describe the purpose of the system:**

ConsularOne is a major system modernization effort intended to replace outdated legacy applications. This modernized system moves paper-based services online, allowing citizens and non-citizens to request services from Consular Affairs (CA). Using a Service Oriented Architecture (SOA), the system decouples service capability to improve performance, scalability, and speed-to-market.

The purpose of the CA CPI is to serve as a common technical infrastructure to provide cross-cutting Consular One services and information technology capabilities to meet CA business

CA CPI

needs. The CPI technology platform has capabilities to support one or more CA business applications to support the administering of consular services. No information is collected by CA CPI; rather, the information in the system comes from the ConsularOne Application and Data (CAD) system. CA CPI includes object storage devices, Oracle Identity, Access Management and common platforms and hardware infrastructure (e.g., VMware, O/S, F5 BIG IP, API Gateway, Storage Area Network (SAN), and Physical Computing Hardware components).

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

- Names of Individuals
- Birthdates of Individuals
- Financial Account Numbers of Individuals/other financial information
- Social Security number
- Phone number(s) of Individuals
- Personal Address
- e-mail address(es) of individuals
- Images or Biometric IDs
- Individual medical information
- Individual education information
- Family information

(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)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C 2651a (Organization of Department of State)
- 22 U.S.C. 3927 (Chief of Mission)
- 22 U.S.C. 211a-218, 2705 (Passports and Consular Reports of Birth Abroad)
- 22 U.S.C. 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- 22 U.S.C. 1731 (Protection to naturalized citizens abroad)
- 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance)
- 22 U.S.C. 2715 (Procedures regarding major disasters and incidents abroad affecting United States citizens)
- 22 U.S.C. 4215 (Notarial acts, oaths, affirmations, affidavits, and depositions; fees)
- Executive Order 11295, of August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)

CA CPI

- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 U.S.C. 6039E (Information Concerning Resident Status)

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

Yes, provide:

- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

State-05 Overseas Citizens Services Records and Other Overseas Records, September 8, 2016
State-26 Passport Records, March 24, 2015

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

This is not applicable because no data is entered into the CA CPI. As noted above, all data stored by the CA CPI is from the CA CAD system. There is no information collected by CA CPI.

(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 Division 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: (obtain info from <http://infoaccess.state.gov/recordsmgmt/recdispsched.asp>)

(If the list is long – name only the top level and indicate length of time as variable based on document and detailed info is at the link)

- Schedule number (e.g., (XX-587-XX-XXX)):
- Length of time the information is retained in the system:
- Type of information retained in the system:

The interfacing Consular One Database Infrastructure (CDI) and the Consular One Applications and Data (CA CAD) are the originating systems where the Consular One PII data is stored. The CDI and CAD PIAs address the applicable Consular One record dispositions of the systems. The CPI main function is to transmit information among the Consular One systems, which may store data temporarily which is replicated in the CCD.

A-15-001-02

American Citizens Services (ACS) system

Description:

The American Citizens Services (ACS) system is an electronic case management application designed to track, monitor, and report on services provided to U.S. citizens traveling or living abroad. ACS supports domestic consular operations and consular activities at overseas Posts.

ACS records include case level data on the following types of citizen services: arrest cases; citizenship issues; death notifications; financial assistance cases; loss of nationality cases; lost and stolen passports; property cases; citizen registrations; and welfare and whereabouts cases. Record level data includes biographic information, case information, and case activity log.

Disposition:

TEMPORARY. Cut off when case closed/abandoned. Destroy 3 years after cut off or when no longer needed, whichever is later.

NOTE: ACS case records are replicated to the Consular Consolidated Database each day for long-term recordkeeping.

(Supersedes NARA Job No. NI-059-96-30, Item 1 and NARA Job No. NI-084-96-4, Item 1)

DispAuthNo:

N1-059-09-40, item 1

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 (are US citizens or aliens lawfully admitted for permanent residence)
- U.S. Government/Federal employees or Contractor employees
- Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

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

Yes No

- If yes, under what authorization?

[26 U.S.C. 6039E](#) – Information Concerning Resident Status

(c) How is the information collected?

CA CPI

Information is collected from within the CA CAD system boundary. All data is transmitted system to system only. The purpose of the CA CPI is to be a shared platform providing cross-cutting business and IT capabilities with a common technical infrastructure leveraged to meet CA business needs.

(d) 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.

(e) What process is used to determine if the information is accurate?

As noted above, no data is entered into CA CPI directly. All data in CA CPI is from the CA CAD as entered by the requestor of service. Accuracy is verified at the point of collection by the CA CAD system which then shares the information with CA CPI.

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

As noted above, no data is entered into CA CPI directly. All data in CA CPI is from the CA CAD as entered by the requestor of service. The information is current and verified at the point of collection by the CA CAD system which then shares the information with CA CPI.

If information needs to be corrected, individuals can make changes via the system of origin (CA CAD).

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

No, the system does not use information from commercial sources or publicly available information.

(h) Is notice provided to the individual prior to the collection of his or her information?

Notice is provided in the CA CAD system, in which information is entered, prior to being transmitted to CA CPI.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? Yes No

- If yes, how do individuals grant consent?

CA CPI

- If no, why are individuals not allowed to provide consent?

This is not applicable because no data is entered into CA CPI directly. The PII processed within CPI is from the CA CAD system. Individuals grant consent via the CA CAD system.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

As noted above, all data stored by the CA CPI is from the CA CAD system. CPI provides the common technical infrastructure supporting information across systems' storage devices to support consular services operations. The PII items listed in paragraph 3(d) are the minimum necessary to facilitate the administering and delivery of consular services.

5. Use of information

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

The purpose of the CA CPI is to serve as a shared platform, providing cross-cutting business and IT capabilities with a common technical infrastructure to support the CA mission. The PII in paragraph 3(d) is used by Consular Affairs to process consular services requested by citizens and non-citizens, such as; visas, passports, and Electronic Consular Reports of Birth Abroad.

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

The purpose of the CA CPI is to be a shared platform providing cross-cutting business and IT capabilities with a common technical infrastructure leveraged to meet CA business needs.

(c) Does the system analyze the information stored in it? Yes No

If yes:

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

N/A

(2) Does the analysis result in new information?

N/A

(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

6. Sharing of Information

CA CPI

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

Information is transmitted and exchanged internally via Department of State Consular One systems.

(b) What information will be shared?

PII listed in paragraph 3d is shared between databases.

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

CA CPI provides the electronic transmission of PII across systems' storage devices to support administering of consular services.

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

All information is encrypted using transport layer security.

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

Communications will be secured using transport and message level security.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Only administrative Database and System Administrators have access to CPI. Privacy concerns regarding the sharing of information focus on two primary sources of risk:

- a. Accidental disclosure of information to non-authorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.
- b. Deliberate disclosure/theft of information regardless whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.
- Strict access control based on roles and responsibilities, authorization, need-to-know, and clearance level.

CA CPI

- System authorization and accreditation process along with continuous monitoring Risk Management Framework (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.
- All communications shared with external agencies are encrypted as per the Department of State's Security Configuration Guides' security policies and procedures.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

For CA CPI, this is not applicable because no data is entered into CA CPI directly. As noted above, all data transmitted by CA CPI is from CA CAD. Individual users do not have access to the system. If individuals need access to their information, they can follow the procedures outlined for the system of origin (CA CAD).

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes No

If yes, explain the procedures.

As noted above, all data transmitted by CA CPI is from the CAD system. Only internal Systems and Database Administrators have access to information. Individual users do not have access to the CPI system, nor is data collected by the CPI system. If corrections are needed to information, individuals can make changes via the system of origin (CA CAD).

8. Security Controls

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

The system is secured within Department of State intranet system, Open Net, where risk factors are mitigated through the use of 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 in order to perform official duties. These users consist of System Administrators and Database Administrators.

CA CPI

Access to the system is secured as follows: All administrative accounts for the system must be approved by the both Government Task Manager (GTM) and Consular Affairs Information Systems Security Officer (CA ISSO).

CA Systems are configured according State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute 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.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

Only System and Database Administrators have access to data in the system. To access the system, persons must be authorized users of the Department of State’s unclassified network, OpenNet, which requires a background investigation and an application approved by the supervisor. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/ Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon to OpenNet.

Access to the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Information System Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user’s particular job function and level of clearance.

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

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with Department of State Security Configuration Guides and conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and Federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g. administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

CA CPI

Access control lists on all OpenNet servers and devices along with Department of State Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with Department of State Security Configuration Guides, auditing is 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; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

Operating System (OS)-Level auditing is set in accordance with the Department of State Security Configuration Guide. The OS interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer and via Splunk. Splunk is the selected log aggregation and analysis platform for CA. It will provide log collection and aggregation across all CST environments, delivering them to a central repository in CA Central Services. It is not part of the CA CPI system boundary. The system log records events logged by the OS interface system components. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, mandatory annual security training, with a privacy component, is required for all authorized users. Each user must complete the Cyber Security Awareness Training annually. The Department's standard "Rules of

CA CPI

Behavior” regarding the use of any computer system and the data it contains require that users to acknowledge (electronically) and agree to the rules and must protect PII through appropriate safeguards to ensure security, privacy and integrity.

- (e) **Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?** Yes No

If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented by the CA ISSO security team to monitor and record possible attempts at unauthorized access.

- (f) **How were the security measures above influenced by the type of information collected?**

The security measures listed above were implemented in accordance with federal laws and Department policies to secure the CPI data due to the sensitivity of information. Organizations or individuals whose PII has been breached or exposed to unauthorized users may include inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. The security measures are in place to minimize that risk, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information.

9. Data Access

- (a) **Who has access to data in the system?**

There are only internal users that have access to the information in the CPI system: System Administrators and Database Administrators.

System and Database Administrators are responsible for the maintenance, upgrades, backups, patches/hotfixes, and database configuration. The access of these administrators is limited to only those database application files necessary to perform daily activities.

- (b) **How is access to data in the system determined?**

Access is role based approved by the supervisor. The user is granted only the role(s) required to perform officially assigned duties.

CA CPI

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? Yes No

Information is documented in the System Security Plan. The Plan includes information regarding system access to data.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Access to the system is limited to system and database administrators in accordance with their assigned roles and responsibilities. Separation of duties and least privilege is employed and users have access to only the data that the supervisor approves to perform official duties.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

-Access control policies and enforcement mechanisms control access to PII.

-Separation of duties is implemented; access is role based as required by policy.

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN). Actions performed while an individual is logged in can be traced to the person that performed the action.