

PRIVACY IMPACT ASSESSMENT

Consular Affairs Security, Infrastructure and Integration Management (CASIIM)

1. Contact Information

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

2. System Information

- (a) **Name of system:** Consular Affairs Security, Infrastructure and Integration Management
- (b) **Bureau:** Consular Affairs (CA)
- (c) **System acronym:** (CASIIM)
- (d) **iMatrix Asset ID Number:** 260352
- (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):** [Click here to enter text.](#)

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 system is currently undergoing its initial Assessment and Authorization (A&A) in order to receive an Authorization to Operate (ATO) status. CASIIM is expected to receive an ATO by May 2018.
- (c) **Describe the purpose of the system:**

CASIIM is a logical business grouping of security and infrastructure support member applications for Consular Affairs, which consists of Oracle Audit Vault and Database Vault (OAVDBV), Consular Affairs Enterprise Service Bus (CAESB) and Threat and Risk Anomaly Sentinel Kit (TRASK). The main purpose of CASIIM is to provide Department of State security officials with auditing, monitoring, reporting and alerting capabilities at the Bureau of Consular Affairs based on Office of the Inspector General (OIG) directives. CASIIM also provides a common structure and method of governance for service offerings as the Department of State moves forward toward its implementation of Service-Oriented Architecture (SOA). This PIA is

written specifically for the CAESB member application which required the PIA. The TRASK and OAVDBV member applications only collect business related PII on members of the Federal workforce. For those systems the System Categorization Form was accepted in lieu of a PIA.

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

- Names of Individuals
- Birthdates of Individuals
- Social Security Numbers (SSN)
- Phone number(s) of Individuals
- Personal Address
- e-mail address(es) of individuals
- Images or Biometric IDs
- Substantive individual medical information
- Medical information of visa applicants

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

- 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. 211a-218 (Passports)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- 22 U.S.C. 2651a (Organization of Department of State)
- Executive Order 11295, August 5, 1996, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 U.S.C. 6039E (Information Concerning Residence Status)
- 22 U.S.C. 3927 (Chief of Mission)
- 8 U.S.C. 1151-1363 (Title II of the Immigration and Nationality Act of 1952, as amended)
- 22 U.S.C. 4084; Public Law 99-570 sec.7361-7362
- 5 CFR part 792
- 22 C.F.R. Parts 40-42, and 46 (Visas)

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

Yes, provide:

SORN Name and Number Date:

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

The information types are not searchable through CAESB as the searches are initiated through the end user applications. CAESB provides data transport services but stores no data.

(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.)

CAESB provides data transport services but stores no data.

If yes provide:

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
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

By use of end-user applications, the CAESB is the official approved CA enterprise transport mechanism for moving data within the Department and to external systems. The ESB provides the CA passport issuance process with a means to check an American citizen SSN against the

Social Security Administration's database in real time to prevent fraud in the passport issuance process.

(c) How is the information collected?

CASIIM does not collect any PII data. CASIIM is a pass through for a multitude of other systems. All PII processed by CASIIM is sourced by systems, including:

- Consular Consolidated Database (CCD) Standalone System
- Front End Processor (FEP) Standalone System
- Consular Lookout and Support System (CLASS) Standalone System
- Non- Immigrant Visa (NIV) Logical Business Group OCSA
- Immigrant Visa Overseas (IVO) Logical Business Group OCSA
- Independent Namecheck (INK) Logical Business Group OCSA
- Travel Document Issuance System (TDIS) Logical Business Group PaSS
- Passport Records Imaging System Management (PRISM) Logical Business Group PaSS
- eMedical
- Consular Electronic Application Center (CEAC)

(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.

Medical information of visa applicants is received via the eMedical system. eMedical is an electronic health processing system that was developed in 2012 by the Australian Government Department of Immigration and Border Protection (DIBP), in conjunction with Citizenship and Immigration Canada (CIC). This system is used for the secure global submission, recording, storage, and processing of Immigration Medical Examinations (IMEs).

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

Data processed by CASIIM is sourced from several systems. CASIIM is dependent upon the validity, safeguards, and accuracy of the PII security controls of the sourcing data systems.

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

Data processed by CASIIM is sourced from several systems. CASIIM is dependent upon the source systems for providing accuracy of the data that passes through the CAESB. Refer to 4.b above for more information.

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

CASIIM does not use any commercial information or publicly available information.

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

CASIIM only processes transactions containing PII that is collected by other systems. CASIIM does not collect PII directly from any users. There is no direct interface nor any opportunity for CASIIM to provide notice to individuals/users.

(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?

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

CASIIM only processes transactions containing PII that is collected by other systems.

CASIIM does not collect PII directly from any users. The ability for an individual to decline providing information that passes through the CAESB is the function of the system using a service on the CAESB.

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

CASIIM only processes transactions containing PII that is collected by other systems all of which have their own privacy and security safeguards.

5. Use of information

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

CASIIM does not maintain data; it only processes transactions containing PII that is collected by other systems. Information transactions are performed by use of service-oriented application and technology infrastructures to achieve business agility through the simplification and enhancement of application-to-application integration.

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

Yes. The PII that passes through the CAESB is used according to the purpose for which the consular systems collecting the information were designed.

(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?

(2) Does the analysis result in new information?

No analysis is conducted by the CAESB.

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

CASIIM only processes transactions containing PII that is collected by other systems.
 CASIIM does not store PII sourced from other systems.

(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

CASIIM only processes transactions containing PII that is collected by other systems.

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

Information is shared internally and externally for fraud assessments and consular adjudications and transactions.

The CAESB transports data to internal consular affairs systems:

- CCD
- CLASS
- FEP
- TDIS

The CAESB transports data as a service to external agencies:

- The government of Canada Immigration and border protection
- The government of Australia's eMedical system
- The Social Security administration

(b) What information will be shared?

CASIIM transports information by processing transactions containing PII data collected by other systems listed in 4b.

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

CASIIM transports information to process transactions containing PII data that is collected by other systems. As noted in 6(a) above, information is shared for fraud assessment purposes, and consular adjudications and transactions.

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

The connections to the CAESB are secured over HTTPS, TLS, and SSL connections. End users utilize certificate client authentication which requires the use of a username and password or CCD authentication to access the data.

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

CASIIM only processes transactions containing PII that is collected by other systems. Accordingly, CASIIM relies upon the safeguards in place in each of those systems to protect the PII. The connections to the CAESB are secured over Hyper Text Transfer Protocol Secure (HTTPS), Transport Layer Security (TLS), and Secure Socket Layers (SSL) connections.

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

The systems that maintain the PII processed by CASIIM have rigorous safeguards in place to protect that data. Access controls and mandatory cybersecurity training are used to reduce the privacy concerns related to CASIIM processing transactions with PII.

7. Redress and Notification

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

CASIIM only processes transactions containing PII that is collected by other systems. Individuals must follow the specific procedures outlined for those systems to gain access to their information.

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

Yes No

If yes, explain the procedures.

If no, explain why not.

CASIIM only processes transactions containing PII that is collected by other systems. CASIIM does not store PII sourced from other systems. Individuals must look to the specific procedures outlined for those systems to correct inaccurate or erroneous information.

(c) By what means are individuals notified of the procedures to correct their information?

Individuals are notified of the procedures to correct their information through Privacy Impact Assessments for the systems sourcing PII to CASIIM, and through the record access procedures outlined in the System of Records Notices of the sourcing systems identified in paragraph 4(c).

8. Security Controls

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

The system is secured within the Department of State intranet 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 their official duties.

Access infrastructure/databases are further protected with additional access controls set at the infrastructure/database level. All system accounts/access must be approved by the user's supervisor. The audit vault system is used to monitor all privileged access to the system and violations are reported to senior management daily, if applicable. Data shared with other government agencies by the source systems collecting the PII is carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), signed by authorizing officers of each agency.

(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.

To access the system, persons must be authorized users of the Department of State's unclassified network 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 PIV/CAC and PIN (Personal Identity Verification/Common Access Card and Personal Identification Number) which meets the dual authentication requirement for federal system access and is required for logon. A system use notification ("warning banner") is displayed before logon is permitted and informs the user of the system use and restrictions with every logon. Users are required to read and actively click a button indicating understanding and agreement before logon can be completed.

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 to be restricted. 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 the CA Security team, periodically scan and monitor information systems for compliance with Bureau of Diplomatic Security (DS) 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's 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.

Access control lists on all OpenNet servers and devices along with Department of State Bureau of Diplomatic Security (DS) 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 DS 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 DS 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. In addition to the security log, the system log and application logs provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. 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.

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

In accordance with Department of State computer security policies, mandatory annual security/privacy training is required for all authorized users including regular refresher training. Each user must complete the Cyber Security Awareness Training annually and pass the Privacy PA-459 course entitled, "Protecting Personally Identifiable Information". The State Department's standard "Rules of Behavior" regarding the use of any computer system and the

data it contains require that users sign that they agree to the rules and that they 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 National Institute for Science and Technology (NIST) Special Publication 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 to monitor and record possible attempts at unauthorized access. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

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

The security measures listed above were implemented to secure the data in the system because the PII data processed by CASIIM is very sensitive. Organizations or individuals whose PII has been breached or exposed to unauthorized users could face 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?

CAESB- System Users; System Administrators, Database Administrators
Oracle SOA Suite Users; Administrators, Deployers, and Monitors

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

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

(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.

Users other than administrators will not have access to all data in the system. 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 access enforcement mechanisms control access to PII.

-Separation of duties is implemented.

-Least Privileges are restrictive rights/privileges or access 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).