PRIVACY IMPACT ASSESSMENT

Management Information System (MIS) PIA

1. Contact Information

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

2. System Information

(a) Name of system: Management Information System

(b) Bureau: Consular Affairs

(c) System acronym: MIS

(d) iMatrix Asset ID Number: #724

(e) Reason for performing PIA: Click here to enter text.

☐ 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 received an Extension of Authorization to Operate (ATO) on May 8, 2017. The authorization is valid until rescinded or the expiry date of July 31, 2019.

(c) Describe the purpose of the system:

The CA Management Information System (MIS) is a web-based reporting tool that tracks predefined productivity statistics of U.S. passport agencies. The CA MIS provides passport system managers the ability to manage passport productivity operations by providing capabilities to query databases and generate a wide number of reports on passport information and statuses specific to any passport agency within the United States. This information includes weekly and monthly workloads on passport production, book inventory, agency hiring summaries, and statistics regarding agency staff.

The CA MIS streamlines the data entry required to produce the reports on management of passports. It is designed to connect to other CA databases to acquire data necessary for reporting on passports, including the ability to assign controlled access to view, run, and schedule reports. The CA MIS helps to manage report cycles through the implementation of a report approval hierarchy by alerting users of due dates, enforcing established submission deadlines, and enabling communication of important messages between Passport Agencies and Field Operations. It includes features and components for a variety of users with differing levels of system privileges to manage passports. Passport Agency administrators are able to access only their own passport agency's reports.

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

- Name
- Personal Phone Number(s)
- Personal Addresses
- Business Addresses
- Personal email addresses
- DoS Personnel Information: Employee name, title, business phone number, Passport Agency/Field Activity

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

- 22 U.S.C 2651a (Organization of Department of State)
- Executive Order 11295, August 5, 1966, 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)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 22 C.F.R. Subchapter F (Nationality and Passports)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- Executive Order 9397, November 22, 1943; Executive Order 13478, November 18, 2008

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

☒Yes, provide:

- SORN Name and Number:
  STATE-26 - Passport Records, March 24, 2015
  STATE-05 - Overseas Citizens Records, and Other Overseas Records, September 8, 2016

☐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 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:
Schedule number, Length of time the information is retained in the system, and Type of information retained in the system:

A-13-001a, b, c &d: Passport Records: Passport and Citizenship Case Files
Description: Case files containing passport applications, Consular Reports of Birth Abroad of U.S. Citizens; Certificates of Witness to Marriage, Applications for Amendment or Extension of Passport; Certificates of Loss of Nationality, and other supporting forms, documents and correspondence pertaining to each case.
DispAuthNo: NC1-059-79-12, N1-059-04-02, N1-059-96-05, respectively

A-15-001-02 American Citizens Service (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.
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
☒ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

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

☐Yes ☒No Not applicable. The MIS does not collect SSNs.

- If yes, under what authorization?

(c) How is the information collected?
No information is entered into MIS by applicants. MIS data is captured from other CA systems (Travel Document Issuance System (TDIS), Passport Lookout Tracking System (PLOTS) and User Manager Web Security (UMWS)).

(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?
MIS information is retrieved from the CA systems listed in paragraph 4(c). Information in these systems is checked for accuracy against submitted documentation, administrative procedures and other CA systems.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
No information is entered into MIS by applicants. Data processed by MIS is retrieved from the CA systems listed in paragraph 4(c). Currency is the responsibility of the individual completing the application for specific services via the CA systems. Applicants can modify or amend records by accessing the website where the record was established in the source CA system. Information can also be updated during the adjudication process for services requested.

(g) Does the system use information from commercial sources? Is the information publicly available?
No, the system does not acquire information from commercial sources nor is it publicly available.

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

N/A. The CA MIS does not collect information directly from the public. Information is provided from other internal databases identified in paragraph 4(c). The notice is provided to applicants upon submission of applications for passport services. All application forms containing PII have Privacy Act Statements stating the purposes for soliciting the information on the form. Additionally, notice of the use of personal information is provided through the two SORNs mentioned above in paragraph 3.f., STATE-26 and STATE-05.

(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?

N/A. The CA MIS does not collect information from the public. The CA MIS receives information from CA systems listed in paragraph 4(c). Individuals grant consent via the passport application processes associated with those systems.

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

The CA MIS does not collect information from the public. MIS receives information from the CA systems addressed in paragraph 4(c).

The Department of State understands the need for PII to be protected. Accordingly, the PII in the CA MIS is handled in accordance with federal privacy regulations. The PII in CA MIS is the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. The PII limited to only what is required for the system to perform the functions for which it is intended to support, providing structured query capabilities on the management and processing of passports.

5. Use of information

(a) What is/are the intended use(s) for the information?
The information is used to generate management reports on information specific to passport agencies and personnel within the United States depicting passport workload statistics and performance. This information includes weekly and monthly workloads, book inventory, agency hiring summaries, and statistics regarding agency staff processing of passports.

(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 information assists in the operations and management of the passport application process.

(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?
(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

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
The information is shared internally within the Bureau of Consular Affairs to include passport agencies and the Passport Services Directorate, and with the Bureau of Diplomatic Security.

- CA MIS acquires passport information from the TDIS and PLOTS systems to generate various management reports.
- CA MIS interfaces with UMWS to acquire user privilege access levels limiting functionality to only authorized roles.
- The CA MIS does not share information externally.

(b) What information will be shared?
Information in paragraph 3.d. and data about passport applicants' status of applications, submission deadlines, data on records of issued and expired passports, not issued applications, and destroyed/stolen/lost passports.

(c) What is the purpose for sharing the information?
The information is shared to assist the Department of State in managing the passport application process to ensure timely processing of passports by monitoring workloads at the passport offices by various management reports on labor and staffing, status of applications, employee productivity and deadlines.

(d) The information to be shared is transmitted or disclosed by what methods?
All information is shared using Department of State approved secure Information System Connection Ports, Protocols and Services. All of the CA systems reside on the Department's secure internal network, OpenNet.

All information is shared internally via systems and accessed by CA personnel to support passport operations. Internal information is shared by direct secured communications (database to database) using transport and message level security interfaces with other Consular Affairs systems.

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

Supervisors along with information system security officers (ISSOs) determine the access level depending on job function and level of clearance.

Information is shared by secure transmission methods permitted by internal Department of State (DoS) policy for the handling and transmission of sensitive but unclassified (SBU) information. Access to electronic files is protected by inherited security controls from the DoS domain infrastructure. All accounts are under the supervision of system managers. Audit trails track and monitor usage and access. Defense in depth is deployed as well as roles assigned based on least privilege. Finally, regularly administered security and privacy training informs authorized users of proper handling procedures.

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

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

1) 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.

2) Deliberate disclosure/theft or information to non-authorized parties regardless whether the motivation was monetary, personal or other.

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

1) 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.

2) Strict role based access control, based on approved roles and responsibilities, authorization, need- to-know, and clearance level.

3) Implementation of management, operational, and technical controls regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

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

The system contains Privacy Act-covered records; therefore, notification and redress are the right of record subjects. Procedures for notification and redress are published in the following System of Records Notices (SORN):

SORN STATE-26: Requests for passport records issued from 1925 to the present should be submitted to the Department of State; Passport Services; Law Enforcement Liaison Division; Room 500; 1111 19th Street, NW., Washington, DC 20522-1705

SORN STATE-05: Requests for Overseas Citizens Records and Other Overseas Records are to be submitted to the Director; Office of Information Programs and Services, A/GIS/IPS; SA-2, Department of State; 515 22nd Street NW., Washington, DC 20522-8100.

Individuals may also visit the Department of State public site and/or the Department of State Privacy Act/FOIA web site for the privacy policy which includes instructions on how to obtain access to records by contacting the listed offices by phone or by mail.

(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.
The CA MIS does not collect information from individuals. Individuals must follow processes of the source systems used to apply for the specific service to request correction of information. Notice to correct personal information is provided at the source site where applicants apply for specific services.

Individuals can also follow procedures outlined in the Passport Records SORNs, STATE-26 and STATE-05 as depicted in paragraph 7(a) above and procedures posted on the Department of State's Privacy website at www.state.gov/privacy.

(c) By what means are individuals notified of the procedures to correct their information?
This is not applicable; the CA MIS does not collect information from individuals. However, notice to correct personal information is provided at the source site where applicants apply for specific services.

Individuals who wish to have their records amended can also find instructions, submission requirements, and the address of the U.S. Department of State, Passport Services, Office of Legal Affairs, Law Enforcement Liaison Division (CA/PPT/S/L/LE) in the Passport Records SORN, STATE-26, posted on the Department of State's Privacy website, www.state.gov/privacy.

8. Security Controls

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

The CA MIS 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 official duties.

All CA MIS 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.

The CA MIS is configured according to 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 and are tracked until compliant or acceptably mitigated.

(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 CA MIS, individuals must be authorized users of the Department of State's unclassified internal network which requires a background investigation and an application approved by the supervisor and Information System Security Officer. 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.

Access to the CA MIS 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. 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?

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State network and respective applications. From that point on, any changes (authorized or not) that occur to data is recorded. In accordance with Department of State Security Configuration Guides, CA MIS 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; or
- Changes in file access restrictions.

The purpose of the CA MIS audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data. If an issue were to arise, administrators of the system would review (audit) the logs that were collected from the time a user logged on until the time he/she signed off. This multilayered approach to security controls greatly reduces the risk that CA MIS PII will be misused.

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

In accordance with Department of State computer security policies, mandatory security (PS800 Cyber Security Awareness) and privacy (PA459 Protecting Personally Identifiable Information) training is required for all authorized users. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. The 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 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.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and reporting, identification and authentication of organizational users, information system monitoring and numerous media controls.

The Information Integrity Branch (IIB) provides administrative life-cycle security protection for the Department of State's information technology systems and information resources. All systems must comply with all guidelines published by Systems Integrity Division, in addition to all Security Configuration Guides published by Diplomatic Security. Adherence to these guides is verified during the system's Assessment and Authorization process.

The CA MIS uses Transmission Control Protocol/Internet Protocol TCP/IP for data transport across the network. Data in transit is encrypted. The TCP/IP suite consists of multiple layers of protocols that help ensure the integrity of data transmission, including hand-shaking, header checks, and re-sending of data if necessary.

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

The information collected contains PII of U.S. citizens and legal permanent residents (LPRs). Due to the sensitivity of information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing.

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above in paragraph 8(e) are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

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

The following personnel have access to these systems: Approved CA MIS DoS Users (Department of State employees and contractors) working domestically and overseas in connection with processing passports; System Administrators and Database Administrators.

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

An individual's job function determines what data can be accessed as approved by the supervisor and the Information Systems Security Officer (ISSO). Access is role based and the 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

Procedures and controls are documented in the System Security Plan. The Plan includes information and procedures regarding access to data in the CA MIS.

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

There are three types of CA MIS user roles: CA MIS Users (Department of State employees and contractors), System Administrators and Database Administrators. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties. To activate, modify or disable user accounts, the Government Manager initiates a request to the Service Desk via an automated access request form.

CA MIS Users- Access to CA MIS is restricted to cleared Department of State direct hire and contractor employees. CA MIS users are assigned access privileges based on their job functions. CA MIS interfaces with UMWS to acquire user privilege access levels limiting functionality to only authorized roles. Access to CA MIS is controlled and managed by the CA MIS System Administrator. The CA MIS account request is reviewed and approved by the user's supervisor and must be approved by the system manager before the request can be granted. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

The System Administrator- The CA MIS System Service and Operations Project Manager completes the Consular Affairs, Consular Systems and Technology (CA/CST) System Administrator request. The Project Manager reviews the role and approves the form authorizing the account to be established and activated, and a current System Administrator creates the account. Database administrators have logon identifications associated with their name that allows for user auditing.

Database Administrators- The CA MIS Database Administrators (DBA) are responsible for the daily maintenance, upgrades; patch/hot fix application, backups and configuration, to the database. CA MIS DBA access is controlled by the Integrated Services (IS) team through the use of access control lists (ACLs) as established by the system administrators. The CA MIS DBAs are authenticated using Windows operating system authentication. The ISSO is responsible for reviewing and approving DBA accounts.

Database Administrators are authorized to access the database for the purpose of performing maintenance, troubleshooting technical issues, and installing software and patches. Database administrators have logon identifications associated with their name that allows for user auditing.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data? CA MIS information is protected by multiple layers of security controls including:

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

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

- CA MIS System Administrators and Database Administrators and internal users have access via OpenNet from the Department of State configured workstations. Users must dual factor authenticate utilizing PIV/CAC and PIN to access data. Users are uniquely identified and authenticated before accessing PII and while logged in can be traced to the person who performed the activity.

- Least Privileges are restrictive rights/privileges or accesses of 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.

- System and information integrity auditing are implemented to monitor and record unauthorized access/use of information.

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing.