PRIVACY IMPACT ASSESSMENT

Passport Records Imaging System Management (PRISM)

1. Contact Information

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

2. System Information

(a) Name of system: Passport Records Imaging System Management (PRISM)
(b) Bureau: Consular Affairs (CA)
(c) System acronym: PRISM
(d) iMatrix Asset ID Number: 896
(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 system is currently undergoing its Assessment and Authorization (A&A) with an expected Authorization to Operate (ATO) status by March 2021.

(c) Describe the purpose of the system:

PRISM provides the capabilities of document scanning, archiving, and image retrieval capabilities for all passport-related documents. Its purpose is to capture images and data from passport documents while also providing centralized access to the archived repository to the passport user community (i.e, authorized Department of State employees) and other system interface stakeholders.

PRISM tracks issued passport applications after they have been shipped back to CA Passport Services, Bureau of Information Resource Management, and Records Management for records processing. The scanning process is performed once the application has been completely processed, meaning that the passport must have undergone adjudication, book printing, and customer delivery before information is scanned into PRISM.

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

Name, date and place of birth, Social Security Number, passport information, race, gender, phone number, personal address, email address, nationality, other names, employer/business contact information, biometrics/images, family information, mother's maiden name, arrests and convictions, and legal 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)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. Sec. 211a-218 (Passport Application and Issuance)
- 22 U.S.C. 2651a (Organization of Department of State)
- 22 U.S.C. 2705 (Documentation of Citizenship
- 22 U.S.C. 3927 (Chief of Mission)
- 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)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 C.F.R. 301.6039E-1 (Information Reporting by Passport Applicants)
- Executive Order 11295, August 5, 1966; (Authority of the Secretary of State in granting and issuing U.S. passports)

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

☒Yes, provide SORN
STATE-26, Passport Records, March 24, 2015
STATE-05, Overseas Citizens Services 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.)

Schedule number/ Department of State Records Disposition Schedule:

A-13-001a,b,c & d: Passport Records; Passport and citizenship Case Files
Description: Case files containing; passport applications, reports of birth of American Citizens Abroad; 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.
Disposition: Records are destroyed or transferred to the Washington National Records Center in accordance with the specific disposition schedule for A-13-001a,b,c & d.
DispAuthNo: NC1-059-79-12, N1-059-04-02, N1-059-96-05 respectively.

A-13-001-23 - Routine Passport Application Status Check and Expedite Fee Upgrades E-mail
Description: Email messages regarding the status of passport applications and requests for expedited service.
Disposition Temporary: Destroy/delete when 25 days old
DispAuthNo: N1-059-98-03, item 1

A-13-002-03 Tracking/Issuance System
Description: Electronic database used for maintenance and control of selected duplicate passport information/documentation
Disposition: Permanent: Delete when twenty-five (25) years old.

DispAuthNo: N1-059-05-11, item 3

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system?

☒ 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
26 C.F.R. 301.6039E-1 (Information Reporting by Passport Applicants)
22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(c) How is the information collected?

PRISM information is collected by either manual entry into the system or scan from paper-based application packages. The information is inputted for document preparation and quality control in preparation for archiving.

(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?

PRISM was developed to scan and track the passport application and images attached to each application for a U.S. passport. Scanning is done only after the application has been completely processed. The passport application must already have undergone adjudication, the passport book printed and delivered to the customer, or the application denied. Manual quality checks are conducted against the submitted documentation at every stage in processing and adjudication of passport applications.

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

The public does not access this system. It is accessible only to State Department personnel with access to the DoS unclassified network accounts on PRISM. PRISM is a repository for processed passport applications and supporting documentation. It is the responsibility of the applicant to ensure the information supplied on passport applications is current. The information is validated throughout the processing of the application and is assumed to be current until such time that the individual fills out a new form to update his/her passport information.

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

PRISM does not use information from commercial sources nor is it publically available.

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

Notice is not provided nor required for the PRISM system. PRISM is not accessible by and does not collect information from the public. Only State Department personnel have access to PRISM. Notice is provided to applicants during the passport application process via the source systems that applicants use to apply.

(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?

PRISM is accessed only by Department of State (DoS) personnel. The paper and online forms completed by applicants via other CA source systems have Privacy Act Statements. Consent is provided when the applicant completes and submits the form via the source system by mail or in person.

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

The PII listed in Question 3(d) is the minimum necessary to perform the actions required by the PRISM system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered and addressed 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 information?

The information in PRISM is used to support decisions regarding applications for passport renewals and stolen 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 PII is used according to the purpose for which the system was designed, which is to provide a repository of scanned passport applications and supporting documentation for management and verification purposes and to support passport application decisions.

(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?
☐Yes
☐No

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

(4) With the new information, will the State 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.

Internal Information Sharing:

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

With that understanding, information in the PRISM system is shared internally with the CA systems Passport Information Electronic Records System (PIERS); Travel Document Issuance System (TDIS); Front End Processor (FEP); Passport Lookout Tracking System (PLOTS); and the User Management Web Security (UMWS) system.

Information in PRISM is not shared externally.

(b) What information will be shared?

All information in paragraph 3(d) is shared internally.

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

Information and images are received and shared with PIERS, TDIS, FEP, PLOT and UMWS as needed for verification processing and management, and for entry into the PRISM repository for archival purposes.

PRISM provides authorized users at domestic passport agencies and overseas posts with the ability to query information pertaining to previously-processed passport applications and vital records data for the purpose of adjudicating applications for passport renewals and lost passports.

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

PRISM is available only on the Department of State intranet, and it is installed on particular CA domain workstations. All connections and data integration endpoints between the CA passport systems are database to database. Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

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

PRISM uses Transmission Control Protocol/Internet Protocol (TCP/IP) to assist with its data transport across the network. The TCP/IP protocol suite consists of multiple layers of protocols that help insure the integrity of data transmission, including hand-shaking, header checks, and re-sending of data if necessary. The transmissions are secured using digital certificates (including web-based Secure Socket Layer (SSL) certificates).

Additionally, controls built into the Department of State intranet, including routers and Network Intrusion Detection Systems (NIDS) provide network level controls that limit the risk of unauthorized access from all Internet Protocol (IP) segments. CA systems that interface with PRISM are strictly controlled by routers and NIDS rule sets that limit ingress and egress to PRISM.

All hard copy records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only.

(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:

a. Accidental disclosure of information to unauthorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic) by personnel having access to PRISM, inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies, in which access to PII could be inadvertently provided unauthorized parties. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information during the end-to-end lifecycle and management of a system duiring its operational use and transmission and sharing of information internally via CA database to database information sharing.

b. Deliberate disclosure/theft of information regardless of whether the motivation was monetary, personal or other.

These risk areas 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. All personnel must also sign a user agreement.

- Strict access control based on roles and responsibilities, authorization and need-to-know.

- System authorization and accreditation process along with continuous monitoring (Risk Management Framework). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management. The implementation of management, operational and technical security controls address and put in place processes for internal sharing of information between and among CA databases, as well as policies and procedures for personnel who have access to CA systems requirements to secure and protect information.

- All communications shared internally database to database are encrypted to protect against either physical or electronic infiltration in accordance with Department of State and Federally mandated security policies and procedures.

7. Redress and Notification

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

Passport applicants do not have access to PRISM or its information. PRISM is a repository for adjudicated scanned passport applications and supporting documentation for use by DoS staff to process passports. However, applicants can follow instructions for gaining access to information as stated in SORNs State-26 and State-05. They may also visit the Department of State public site for the privacy policy which includes instructions on how to obtain access 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.

Passport applicants do not have access to PRISM or its information. PRISM is a repository for adjudicated scanned passport applications and supporting documentation for use by DoS staff to process passports. However, during the passport application process applicants can follow instructions for requesting changes to their information as stated in SORNs State-26 and State-05. They may also visit the Department of State public site for the privacy policy which includes instructions on how to request changes by contacting the listed offices by phone or by mail.

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

PRISM is not a public-facing application and passport applicants do not have access to PRISM or its information. However, applicants are notified during the passport application of procedures to correct the information stored in PRISM by a variety of methods:

1. Through procedures published in the applicable SORNs
2. Through procedures provided in the link on web pages to the Department of State Privacy Policy
3. By following instructions on forms or web pages where the data were inputted
4. By notifying the Department of State by letter or email that a correction is needed

Each method contains information on how to amend records, who and what office to contact, and contact information.

If no, explain why not.

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 to applications/databases are further protected with additional access controls set at the application/database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer (ISSO). The audit vault system is used to monitor all privileged access to the system and any violations are reported to senior management daily.

Applications are configured according the State Department Security Configuration Guides to optimize security while still providing functionality. 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.

(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 PRISM, persons must be authorized users of the Department of State's internal unclassified network which requires a background investigation and an application approved by the supervisor and the local ISSO. Only DoS personnel who have completed completed the annual Passport Data Security Awareness (PC441) course can access PRISM. Additionally, 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 system is role-based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and access to information 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 Department of State Bureau of

Diplomatic 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.

Access control lists on all OpenNet servers and devices along with Department of State Bureau of Diplomatic Security, Security Configuration Guides 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.

Every PRISM database server is configured in accordance with Department of State Security Configuration Guidelines on auditing to enable tracking of events at the database levels such as:

- Multiple logon failures; log off successes;
- 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.
The PRISM Operating System (OS)-level auditing is set in accordance with the Diplomatic Security, Security Configuration Guides. The OS interface allows the system administrator or local 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. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name.

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

In accordance with Department of State computer security policies, mandatory Cyber Security Awareness training (PS800) is required for all users of State Department systems. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. State Department personnel are also required to take the biennial privacy training course, Protecting Personally Identifiable Information (PA318). This course provides refresher training on the Privacy Act, Personally Identifiable Information (PII) and proper handling of PII. The Passport Services Internal Control Guide requires all passport personnel (government and contractors) to complete the Passport Data Security Awareness (PC441) course as an annual recertification to maintain access to PRISM. This course provides refresher training on the Privacy Act, Personally Identifiable Information (PII) and proper handling of PII.

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 acknowledge and agree to the rules and to 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 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 information collected, if exposed to unauthorized users, may cause inconvenience, distress, or damage to standing or reputation, financial loss, harm to State Department programs or the public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violation. The security measures listed above were implemented to secure the data in the system in accordance with federal laws and policies, including Department policies.

9. Data Access

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

PRISM OpenNet Users, System/Web Administrators and, Database Administrators.

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

Access is determined based on requests which are approved by the supervisor and the local 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

Information is documented in the PRISM 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.

Separation of duties and least privilege is employed and users have access to only the data that the supervisor and the local ISSO approves to perform official duties.

- PRISM OpenNet Users consist of Agency Clerk, Agency Processing Managers, and Help Desk Personnel. PRISM OpenNet Users having access to PRISM are granted specific database privileges to perform their specific job function.

    - Agency Clerk: Has access to all information in PRISM to perform specific quality management functions.

    - Agency Processing Manager: Has access to all information in PRISM to perform all quality management functions.

    - Help Desk: Can view inquiry screen, can view and access certain information to perform helpdesk functions.

    - Helpdesk Read only: Can only view certain information in PRISM to perform helpdesk functions.

    - System/Web Administrators: PRISM System/Web Administrators have access to all data in the respective web application servers to perform daily maintenance, establish access control lists (ACLs), and perform backups of the system. The local Post (ISSO) authorizes the establishment, activation, modification, review, disabling, and removing of all PRISM System/Web Administrator accounts.

    - Database Administrators: PRISM Database Administrators (DBA) have access to all data in the PRISM database and are responsible for the daily maintenance, upgrades, patch/hot fixes, backups and configuration to the database. DBA access is controlled by the Integrated Services (IS) team through the use of ACLs as established by the system administrators. PRISM DBAs are authenticated using Windows operating system authentication.

(f) 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; 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).

-Privacy training informs users of the Rules of Behavior and warns against unauthorized browsing.