PRIVACY IMPACT ASSESSMENT

Passport Data Interchange Transfer System (PDITS) PIA

1. Contact Information

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

2. System Information

(a) Name of system: Passport Data Interchange Transfer System (PDITS)

(b) Bureau: Consular Affairs

(c) System acronym: PDITS

(d) iMatrix Asset ID Number: 5227

(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 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 The authorization is valid until rescinded or the expiry date of July 31, 2019.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:

PDITS

The Passport Data Interchange Transfer System (PDITS) is a consolidation of database functionality and support under one design, development, and management structure. PDITS interfaces with the Travel Document Issuance System (TDIS) and Online Passport Status Service Structured Query Language (OPSS SQL). Prominent associations include being the recipient and repository of all issued passport data from TDIS. OPSS SQL is a database that stores information that is retrieved from PDITS for updates. PDITS's mandate is to

continually ensure data quality and integrity in the passport databases, particularly with respect to the data imported from TDIS.

There are no external information sharing partners within the PDITS environment.

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

PDITS receives the following PII as a data transfer from TDIS. TDIS obtains the information from passport books and passport cards, applications for passport books and passport cards, amendments, extensions, replacements, and/or renewals of passport books or cards. The information in PDITS is not collected from the applicant. Although the form DS 4085 is no longer accepted for requesting additional visa pages, the form is still in the system and used for other purposes such as miscellaneous actions, and collects the same PII.

- Applicant's name
- Date of birth
- Place of birth
- Gender
- Social Security Number
- Biometric IDs
- Legal and family information
- Mailing address
- Email address
- Phone numbers

(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, 2705 (Passports and Consular Reports of Birth Abroad)
- 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. Parts 50 and 51 (Nationality Procedures and Passports)
- 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)

(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

☐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-13-001-16 Passport Lookout Master
Description: This on line information system assists Passport Services staff in determining those individuals to whom a passport should be issued or denied, identifies those individuals who have been denied passports, or those who are not entitled to the issuance of full validity passport and those whose existing files must be reviewed prior to issuance.
Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 16)
DispAuthNo: N1-059-04-2, item 16

A-13-002-02 Requests for Passports
Description: Copies of documents relating to selected passport requests.
Disposition: Temporary: Cut off at end of calendar year. Hold in current file area and retire to Records Service Center when 2 years old. Destroy/delete when twenty-five (25) years old.
DispAuthNo: N1-059-05-11, item 2

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? 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

- If yes, under what authorization?
26 U.S.C. 6039E (Information Concerning Resident Status) and
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?
PDITS receives the PII as a data transfer from TDIS. The general public does not have access to PDITS. All data is transmitted system-to-system only from TDIS to PDITS.

TDIS obtains the information from passport books and passport cards, applications for passport books and passport cards, amendments, extensions, replacements, and/or renewals of passport books. The passport information is collected when an applicant fills out an application for a passport and/or passport card or other passport services offered.

(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?
No data is entered into PDITS directly. All data in PDITS is transferred from TDIS. TDIS quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimize instances of inaccurate data. OPSS pulls data from PDITS for updates.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
No data is entered into PDITS directly. Information is transferred from TDIS to PDITS.

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

No, the system does not get information from commercial sources, nor is the information publicly available.

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

Not applicable because no data is entered into PDITS directly. The notice is provided to applicants upon submission of applications for passport services. All data transmitted by the PDITS system is from the TDIS system. Individuals grant consent via the passport application process.

(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?

No data is entered into PDITS directly. All data transmitted by the Consular Affairs (CA) PDITS system is from the TDIS system. Individuals grant consent via the passport application process where information is included in the source CA system for the requested services.

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

The Department of State understands the need for PII to be protected. Accordingly, the PII in PDITS is handled in accordance with federal privacy regulations regarding the collection, access, disclosure, and storage of PII. PDITS only collects the information necessary for the processing and management of passport applications.

5. Use of information

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

PDITS
PDITS receives PII (information from passport books and passport cards, applications for passport books and passport cards, amendments, extensions, replacements, and/or renewals of passport books or cards) from TDIS to electronically verify and validate passport information collected by the Department.

(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 relates to resolving passport application processing issues 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.

PDITS is the recipient and repository of all issued passport data from TDIS, including the PII identified in paragraph 3.d. OPSS SQL is a database that stores information that is retrieved from PDITS for updates.

PDITS does not connect to any external information system or allow access from external systems. Information is not shared with any external organizations.

(b) What information will be shared?
The PII in paragraph 3.d. is shared internally and is about passport applicants, in addition to the status of applications, all records of issued and expired passports, not issued applications, and destroyed/stolen/lost passports.

(c) What is the purpose for sharing the information?
Information is shared internally to assist the Department of State in managing the passport application process.

(d) The information to be shared is transmitted or disclosed by what methods?
All internal information is shared using Department of State approved Information System Connection Ports, Protocols and Services.

Internal information is shared by direct secured communications (database to database) using transport and message level security interfaces with other Consular systems.

(e) What safeguards are in place for each internal or external sharing arrangement?
Recipients within the Department of State must comply with U.S. government requirements for the protection and use of PII. Information is shared by secure transmission methods in accordance with Department of State policy for the handling and transmission of sensitive but unclassified information. Access to electronic files are protected by inherited security controls from the DoS domain infrastructure.

Defense in depth layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring are deployed, as well as role based access based on least privilege.

(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) deliberate disclosure/ theft of information regardless of whether the motivation was monetary, personal or other; 2) 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.

The Department of State mitigates these risks by enforcing rules and requirements regarding:

- Frequent, regular 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;
- Strict access control based on roles and responsibilities, authorization and need-to-know;
- 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?
For PDITS, this is not applicable because no data is entered into CA PDITS directly. As noted above, all data transmitted by CA PDITS is from CA TDIS. 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 TDIS).

Notices to individuals on how to access their information are provided at the point of collection of information for the system where services are being requested. Procedures for notification and redress are also published in the System of Records Notice (SORN) Passport

Records – STATE-26, Overseas Citizens Records, STATE-05, and in rules published within 22 CFR 171.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☐Yes ☒No

All data transmitted by CA PDITS is from CA TDIS. Only internal system users and Database Administers have access to information. The public does not have access to the CA PDITS, nor is data collected by PDITS from the public. If corrections are needed to information, individuals can make changes to correct information via the system of origin where the information is captured.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
Individuals who wish to have their records amended can 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, the Overseas Citizens Records - STATE-05 and in rules published within 22 CFR 171.

8. Security Controls

(a) How is the information in the system secured?
The PDITS 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 official duties.

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

(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 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 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?

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 are recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; 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. 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 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, PDITS users are required to complete the annual Cyber Security Awareness Training and the Privacy Act PA 459 course, Protecting Personally Identifiable Information. 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.

Bureau of Diplomatic Security (DS) guidelines are implemented for operating systems, web servers, and databases to prevent unauthorized disclosure of information and detect changes to information during transmission.

Systems use Transmission Control Protocol/Internet Protocol TCP/IP to assist with its data transport across the network. 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. Additionally, systems employ the use of Hash message authentication codes to sign packets verifying that the information received by the system from the Internet is exactly the same as the information sent. Also, the Systems Integrity Division is responsible for developing policies regarding digital certificates (including web-based Secure Socket Layer (SSL) certificates), and all cryptographic keys.

The Information Integrity Branch (IIB) provides administrative life-cycle security protection for the Department of State's information technology systems and information resources. IIB's goal is to ensure that information processed and stored is safe from unauthorized access, disclosure, disruption, or denial of service. The IIB is composed of four operational elements:

- Antivirus
- Mainframe Security
- The Public Key Infrastructure (PKI) and Biometrics
- E-Authentication

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.

(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 (LPR). Passport information and the PII contained therein constitute the substantive portion of the information contained in PDITS. 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 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:
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 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
Consular Affairs/Consular Systems and Technology (CA/CST) adheres to a formal, documented audit and accountability policy that addresses purpose, scope, roles, and responsibilities. In addition, there are documented procedures to facilitate the implementation of the policy and the audit and accountability controls.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
There are two types of PDITS user roles: System and Database Administrators. Separation of duties and least privilege are employed and users have access to only the data that the supervisor, Information System Government Technical Manager and ISSO approves to perform official duties.

The System Administrator- The System Service and Operations Project Manager complete the CA/CST System Administrator Account Request Form. The Project Manager signs the form authorizing the account to be established and activated, and a current System Administrator creates the account.

Database Administrators- Database Administrator (DBA) access is controlled by the Data Integrated Services (IS) team. PDITS DBA is authenticated using Windows operating system authentication only. The Information System Government Technical Monitor is responsible for reviewing and approving accounts. The current DBA activates/establishes an account when he/she adds the new user to the Windows security group. Access is disabled when no longer required; accounts are reviewed every 60 days to determine when access should no

longer be granted.

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

PDITS information is protected by multiple layers of security controls including network security, Department site physical security and management security.

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing. Audit logs are reviewed at the Database and System level as follows:

System Administrators and Database Administrators accounts within PDITS are audited for access to PDITS data processing functions using their privileged accounts. PDITS is configured to audit any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information.

Database level: The System Security Officer (SSO) reviews the Structured Query Language (SQL) logs for indications of inappropriate or unusual activity on the PDITS database, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

System level: The SSO reviews the Operating System (OS) logs for indications of inappropriate or unusual activity of systems, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.