PRIVACY IMPACT ASSESSMENT

Passport Data Interchange Transfer System (PDITS)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: November 2022
(b) Name of System: Passport Data Interchange Transfer System
(c) System acronym: PDITS
(d) Bureau: Consular Affairs (CA)
(e) iMatrix Asset ID Number: 5227
(f) Child systems (if applicable) iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

☐ New system
☐ Significant modification to an existing system
☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?

☒ Yes ☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?

☒ Yes ☐ No

If yes, has the privacy questionnaire in Xacta been completed?

☒ Yes ☐ No

(c) Describe the purpose of the system:

The Passport Data Interchange Transfer System (PDITS) is a consolidation of database functionality and support under one design, development, and management structure. PDITS passport archive is a centralized backend system that stores passport data once a product has been issued or the application is considered completed. PDITS interfaces with two other Consular Affairs systems, the Travel Document Issuance System (TDIS) and the
Online Passport Status Service (OPSS) system. Prominent associations include being the recipient and repository of all issued passport data from TDIS. The OPSS system 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.

(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.

- Name
- Date of birth
- Place of birth
- Mailing address
- Personal Email address
- Personal Phone number
- Citizenship
- Social Security Numbers (SSN)
- Biometric records/IDs (Facial recognition)

(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)
22 U.S.C. 2651a (Organization of Department of State)
18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
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, etc.)?

☑ Yes, provide:
   SORN Name and Number: Passport Records, STATE-26
   SORN publication date: 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 Office 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 (Consolidate as much as possible):

**Schedule number:** A-13-001-16 Passport Lookout Master  
**Disposition Authority Number:** N1-059-04-02  
**Length of time the information is retained in the system:** Destroy when active agency use ceases. (ref. N1-059-96-5, item 16)  
**Type of information retained in the system:** This online 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.

**Schedule number:** A-13-002-02 Requests for Passports  
**Disposition Authority Number:** N1-059-05-11, item 2  
**Length of time the information is retained in the system:** Temporary. Delete when twenty-five (25) years old.  
**Type of information retained in the system:** Copies of documents relating to selected passport requests.

**Schedule number:** A-13-002-03 Tracking/Issuance System  
**Disposition Authority Number:** N1-059-05-11, item 3  
**Length of time the information is retained in the system:** Temporary. Delete when 25 years old.  
**Type of information retained in the system:** Electronic database used for maintenance and control of selected duplicate passport information/documentation

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) On what other entities above is PII maintained in the system?
Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) **If the system contains Social Security Numbers (SSNs), is the collection necessary?**
☒ Yes  ☐ No  ☐ N/A

- 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)

(d) **How is the PII collected?**

PDITS receives the PII as a data transfer from TDIS. The applicant completes the required form for a passport or passport renewal either through a paper form or online via a CA source system, where information is uploaded to TDIS and transmitted to PDITS.

(e) **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.

(f) **What process is used to determine if the PII is accurate?**

All data in PDITS is transferred from TDIS. Accuracy of the information on passport applications and supporting citizenship evidence is the responsibility of the passport applicant. Prior to information being transmitted to PDITS, quality checks are conducted against the submitted documentation at every stage of the passport process by Department of State analysts, in addition to information being cross-checked with other CA systems to minimize instances of inaccurate data.

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

Yes, the information is current. All data in PDITS is transferred from TDIS. TDIS quality checks are conducted against the submitted documentation at every stage for currency. It is the responsibility of TDIS to ensure that the information remains current.
(h) Does the system use information from commercial sources? Is the information publicly available?

No. PDITS does not use commercial sources of information nor is the information publicly available.

(i) How was the minimization of PII in the system considered?

The PII listed in 3d is the minimum necessary to perform the actions required by the PDITS. Concerns about collecting and maintaining PII 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. Impact is minimized as collection of PII is limited to only what is required for PDITS for the processing and management of passport applications.

5. Use of information

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

All PII in PDITS is transferred from TDIS. Information in PDITS is pulled and used by OPSS to provide updates to its database to provide quick status information of passports of applicants, e.g., when the passports will be produced and emailed.

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

Yes. PDITS mandate is to retrieve and store up-to-date passport information, while ensuring data quality to support the OPSS operations in providing quick passport updates of applicants.

(c) Does the system analyze the PII stored in it? ☐ Yes ☒ No

If yes:
1. What types of methods are used to analyze the PII?

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

(d) If the system will use test data, will it include real PII? ☐ Yes ☐ No ☒ N/A

If yes, please provide additional details.
6. Sharing of PII

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

Internal: The term “internal sharing” traditionally refers to the sharing of information within the Department of State, but external to the owning organization (referred to as “bureau” at the Department of State). However, since the various Bureau Consular Affairs offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau. With that understanding, information in PDITS is shared with the Online Passport Status Service (OPSS) system.

External: Information is not shared externally.

(b) What information will be shared?

Internal: All PII in 3d is shared with the OPSS system.

External: N/A

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

Internal: Information is shared with the OPSS system to assist in managing the passport application process by providing quick status information of passports of applicants, e.g., when the passports will be produced and emailed.

External: N/A

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

Internal: All information is shared internally database to database and is encrypted using Secure Socket Layer (SSL) and transport layer security (TLS).

External: N/A

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

Internal: The PDITS system safeguards entail secure protocol connections (Hypertext Transfer Protocol Secure (HTTPS)) which provides secure encryption interfaces. The Department of State security program involves the establishment of strict rules of behavior outlined in the security controls for each major application, including PDITS. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability and data integrity. In
PDITS

addition, to access electronic files, Department employees must have a Personal Identity Verification/Personal Identification Number (PIV/PIN), as well as a separate password to access PDITS data. Audit trails track and monitor use and access of systems that reside on the Department’s intranet network, OpenNet.

External: N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

PDITS information is obtained from TDIS. When the collection of information by the source system involves potential PII collected on U.S. citizens, there is a Privacy Act Statement displayed on the form in which the applicant is seeking a consular service, such as a passport. It is the responsibility of the source system to provide notice to U.S. persons when collecting PII submitted via CA source systems.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐ Yes ☒ No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

The public does not have access to the PDITS, nor is data collected by PDITS directly from the public. Information in PDITS is obtained from TDIS. Consent is acquired via the CA source system where the applicant applied for services.

(c) What procedures allow record subjects to gain access to their information?

The public does not have access to the PDITS, nor is data collected by PDITS directly from the public. Information in PDITS is obtained from TDIS. Where applicable, record subjects can gain access to their information via the CA source system where the applicant applied for services. Also, the System of Records Notice (SORN) STATE-26, Passport Records, includes procedures on how to contact an office to access records pertaining to the individual.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒ Yes ☐ No

If yes, explain the procedures.
The public does not have access to the PDITS, nor is data collected by PDITS directly from the public. If corrections are needed, individuals can make changes to correct information via the source system of origin where the information is captured. Individuals can also follow the record access procedures in SORN STATE-26, which include procedures on how to contact an office for assistance in addressing inaccurate information.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

The public does not have access to the PDITS, nor is data collected by PDITS directly from the public. If corrections are needed to information, individuals can make changes to correct information by following procedures in the source system. Individuals can also follow procedures in SORN STATE-26, which points to necessary procedures individuals must follow to correct their information. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated with the form which the applicant is seeking a consular service.

8. Security Controls

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

The PDITS is secured within the Department of State intranet which mitigates risk factors through defense-in-depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring.

The PDITS is configured according to the Department of State 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. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need to perform official duties.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Access to the PDITS is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. Department of State PDITS users, system administrators and database administrators have access to PDITS based on prescribed roles to conduct required business and assigned roles to support the management and execution of the passport program. PDITS users consist of both government and contractor cleared and approved personnel.
(c) Describe the procedures established to limit system and data access to only those individuals who have an “official” need to access the information in their work capacity.

Separation of duties and least privilege access are employed; users have access to only the data that the supervisor and local Information System Security Officers (ISSOs) approve to perform official duties. Access is role-based, and the user is granted only the role(s) required to perform officially assigned duties.

Least privileges are restrictive rights/privileges or access users need for the performance of specified tasks. The Department of State ensures through least privileges principles 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) necessary to perform their job duties. Users are uniquely identified and authenticated before accessing PII.

(d) How is access to data in the system determined for each role identified above?

Access to PDITS is limited to authorized Department of State users, including cleared contractors who have a justified need for the information to perform official duties. All roles have been analyzed to determine the specific data set and corresponding functions that will be required in accordance with the person’s job and level of security approved by the supervisor and the local Information System Security Officer. Accordingly, when a user or service account is added to a particular database role, access is limited to only the data and functions allotted.

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

The PDITS CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with Department of State Security Configuration Guides, conduct annual control assessments (ACA) to ensure systems 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 systems, including PDITS for changes to the Department of State mandated security controls. Access control lists on OpenNet servers and devices along with Department of State Security Configuration Guides standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures.

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

- Multiple logon failures;
PDITS

- 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.

(f) **Are procedures, controls, or responsibilities regarding access to data in the system documented?**

☒ Yes ☐ No

The PDITS System Security Plan (SSP) contains the procedures, controls, and responsibilities regarding access to data in the system.

(g) **Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.**

All system administrators must take the IA210 System Administrator Cybersecurity Foundations Course which has a privacy component. In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially.

The Department of State’s standard “Rules of Behavior” regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy, and integrity.

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 PDITS. This course provides refresher training on the Privacy Act, Personally Identifiable Information (PII) and proper handling of PII.