1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: August 28, 2008

(b) Name of system: Passport Information Electronic Records Systems

(c) System acronym: PIERS

(d) IT Asset Baseline (ITAB) number: 85

(e) System description (Briefly describe scope, purpose, and major functions):

PIERS is a business application that makes it possible to search and view passport records. In addition, images of passport records are available in PIERS via the Passport Records Imaging System Management (PRISM) database. Although PRISM is listed as a separate database, PIERS presents both the data and the image as one record. These systems are accessible through the Consular Consolidated Database (CCD).

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): Not applicable

(h) Date of previous PIA (if applicable): March 7, 2006

3. Characterization of the Information

The system:

☐ Does NOT contain PII.

☒ Does contain PII.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

Passport applicant information is imported into PIERS from a separate Consular Affairs computer system, and is initially collected on any of these forms submitted by the applicant:

- Form DS-11 is used for passport applications from first time applicants.

- Form DS-82 is for persons applying to replace a passport issued within the past 15 years, who are over the age of 16 when the passport was issued, and who also provide the old passport with the application form.
- Form DS-5504 is for persons replacing a passport that was issued less than a year earlier. The form may be used to replace an emergency passport with a full validity one; to make a change to the applicant's identifying information (e.g., name change due to marriage or court order); or to correct a printing error in their passport.
- Form DS-4085 is used to add visa pages to a previously issued and currently valid passport.
- Form DS-10 is used in conjunction with a DS-11 when an acceptable birth certificate cannot be obtained for a person born in the United States.
- Form DS-60 is used in conjunction with a DS-11 when the name which is used by the applicant is (1) substantially different from that shown on the evidence of citizenship or (2) has been adopted without formal court proceedings and was not acquired by marriage.
- Form DS-64 is used in conjunction with a DS-11 when a previous valid or potentially valid U.S. passport cannot be presented.
- Form DS-71 is used in conjunction with a DS-11 only when the applicant for a passport is unable to establish his or her identity to the satisfaction of a person authorized to accept passport applications.
- Form DS-86 is used when passport applicant does not receive the U.S. passport card and/or passport book for which he or she applied.
- Form DS-3053 is used in conjunction with a DS-11 if a non-applying parent or guardian consents to the issuance of a passport for his or her minor child that is younger than 16 years old.

The above forms may be completed by the applicant on published paper forms available at many government office locations or may be completed online using web forms at the Department of State's public web site. If web forms are used, the applicant must still print the form and submit it as hardcopy with supporting documents.

b. How is the information collected?

PIERS collects data from the Travel Document Issuance System (TDIS) and Passport Records Imaging Management System (PRISM). PIERS provides access to archived passport applications, including those resulting in denials or restricted travel passports. All currently valid passports and expired passports have scanned passport application images available.

c. Why is the information collected and maintained?

The purpose of PIERS is to provide authorized users at domestic passport agencies and overseas posts with the ability to query information pertaining to previously processed passport applications and vital record data. PIERS provides structured query capabilities to the archived data it maintains.

d. How will the information be checked for accuracy?

Accuracy of the information on a passport application and submission of citizenship evidence is the responsibility of the passport applicant. Quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimize instances of inaccurate data.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The following authorities provide for the administration of the program supported by PIERS:

- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports)
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a–218, 2651a, 2705
- 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. 1185 (Travel Control of Citizens)

4. Uses of the Information

a. Describe all uses of the information.

PIERS provides authorized users at both domestic agencies and overseas posts with the ability to query information pertaining to passports and vital records, as well as to request original copies of the associated documents. PIERS provides case-based and user-defined views of the information and supports electronic tracking and reporting of the work process.

b. What types of methods are used to analyze the data? What new information may be produced?

PIERS records are generally retrieved by individual name, application number, passport book number, or passport card number. Authorized users have the additional ability to create and modify passport records and vital records. Records can be corrected to maintain data integrity. PIERS also supports the production of a variety of statistical reports.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

No commercial information, publicly available information, or information from other Federal agency databases is used in PIERS. All of the information in PIERS is derived from passport applications and vital records collected and maintained by Consular Affairs.

d. Is the system a contractor used and owned system?

PIERS is a government system. It is supported by contract employees, some of whom are located at contractor-owned facilities. Direct-hire U.S. government employees have the sole responsibility for adjudicating passport applications to determine if applicants are U.S. citizens and qualify for passport issuance. Contractors support government employees by entering data, printing and mailing passports, and answering customer service inquiries.

Contractors involved in the passport fulfillment process (i.e., data entry, scanning, or correction of records or the printing and mailing of passports) are subjected to a background investigation by the contract employer equivalent to a “National Agency Check” of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of PIERS hardware or software must have at least a Secret-level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor-owned facilities are annually inspected by Diplomatic Security.

5. Retention

How long is information retained?

Retention of these records varies depending on when the passport application was received. They are retired or destroyed in accordance with published record schedules of the Department of State and as approved by the National Archives and Records Administration. The established retention period for electronic records in PIERS is presently 100 years.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The Bureau of Consular Affairs oversees a network of facilities that may internally share or disclose the personal information collected and maintained in PIERS. These facilities include over a dozen regional passport agencies, a special issuance agency, three national processing facilities, the National Passport Information Center, and the Headquarters offices in Washington, DC. United States embassies and consulates abroad also accept passport applications. Information is shared within these entities only for the purpose of issuing or denying a passport, subject to the law.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Passport information maintained by Consular Affairs may be disclosed to external agencies under the authority of routine uses published in the Privacy Act system of records titled STATE-26, Passport Records. PIERS operates in tandem with TDIS and provides access to a small subset of passport-related documents, typically only the applicant's passport application form including photograph. In complex circumstances (e.g., suspicion of fraud) additional information is accessible through PIERS. These cases represent a small percentage of all records in PIERS.

Under the above arrangement, PIERS is more commonly the system from which passport records are disclosed in a manner consistent with a published routine use. The principal purposes of disclosures outside the Department of State include:

- Department of Homeland Security for border patrol, screening, and security purposes; law enforcement, counterterrorism, and fraud prevention activities;
- Department of Justice, including the Federal Bureau of Investigation, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. Marshals Service, and other components, for law enforcement, counterterrorism, border security, fraud prevention, and criminal and civil litigation activities;
- Internal Revenue Service for the current addresses of specifically identified taxpayers in connection with pending actions to collect taxes accrued, examinations, and/or other related tax activities;
- National Counterterrorism Center to support strategic operational planning and counterterrorism intelligence activities;
- Office of Personnel Management (OPM), other federal agencies, or contracted outside entities to support the investigations OPM, other federal agencies, and contractor personnel conduct for the federal government in connection with verification of employment eligibility and/or the issuance of a security clearance;
- Federal, state, local or other agencies for use in legal proceedings as government counsel deems appropriate, in accordance with any understanding reached by the agency with the U.S. Department of State;
- Assistance to parents of underage minors;
- Upon request of attorneys representing an individual in administrative or judicial passport proceedings when the individual to whom the information pertains is the client of the attorney making the request;
- Members of Congress when the information is requested on behalf of or at the request of the individual to whom the record pertains;
- Foreign governments, to permit such governments to fulfill passport control and immigration duties and their own law enforcement, counterterrorism, and fraud prevention functions, and to support U.S. law enforcement, counterterrorism, and fraud prevention activities; and
- Government agencies other than the ones listed above that have statutory or other lawful authority to receive such information on a need-to-know basis.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information is shared with external agencies by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Access to the information by external agencies is based upon agreements with those entities as to how they will use the data and protect it in accordance with the Privacy Act.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

The information in this system is covered by STATE-26, Passport Records, which was last amended January 8, 2008, at 70 FR 1660-1664.

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notice titled STATE-26, Passport Systems.

b. Do individuals have the opportunity and/or right to decline to provide information?

No. Once an applicant applies for a passport, their record is maintained in PIERS until the records retention schedule requires its destruction.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. Once an individual applies for a passport, their record is maintained in PIERS until the records retention schedule requires its destruction.

9. Notification and Redress

What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

PIERS contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to PIERS is limited to authorized Department of State staff having a need for the system in the performance of their official duties. All authorized government users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to PIERS requires a unique user account assigned by Consular Affairs.

Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes a rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g., curiosity browsing). Completed applications are also reviewed and approved by the information system security officer (ISSO) prior to assigning the logon.

External agencies access PIERS through CCD and require a separate user account managed by Consular Affairs.

The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly in order to retain access.

11. Technologies

What technologies are used in the system that involve privacy risk?

PIERS operates under standard, commercially-available software products residing on a government-operated computing platforms not shared by other business applications or technologies. No technologies commonly considered to elevate privacy risk are employed in PIERS.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates PIERS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, its most recent date of authorization to operate was June 30, 2006.