1. Contact Information

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

2. System Information

(a) Date PIA was completed: March 1, 2010

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

(c) System acronym: PIERS

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

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

The Passport Information Electronic Records System (PIERS) is a suite of web (that provides structured query capabilities to the data maintained within its environment) and desktop applications for managing passport records, Consular Reports of Birth Abroad (CRBA), Certificate of Witness to Marriage (CWM), Records of Death (ROD), Advance Finder (AF), Diplomatic and Official Tracking System (DOTS), Monitor, and Panama Canal Zone (PCZ) data. It operates on the Department of State's OpenNet network. It provides direct access for OpenNet users at Agencies, Departments and Record services and, indirect access for external users through the Consular Consolidated Database (CCD).

The PIERS system provides its users with both case-based and user-based views of information, and support for electronic checking and reporting of work processes. Case-based views refer to the different types of data records that the PIERS system and database maintain. This includes passport information (all records of issued and expired passport, not issued applications, and destroyed/stolen/lost passports) and Consular records of overseas births and deaths. User-based views refer to the PIERS systems ability to provide access to different data elements, record types, and system functions based on specific groups or system application roles assigned to individual users.

(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):

(h) Date of previous PIA (if applicable): August 28, 2008

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

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

The PII elements collected are the applicant's surname, date of birth, address, telephone number, social security number, passport, driver's license or other identifying number(s), education, financial transactions, employment, medical or any other identifying attribute assigned to the individual. The source of the information provided to PIERS is the passport applicant. Information is collected from the passport applicant and input into TDIS. It is then transferred via the Front End Processor (FEP), which communicates with PIERS to create new records and modify the records, and Datashare, which feeds data to PIERS. The data includes an approved passport application from the Post repository server, which is in place for the sole purpose of supplying OPSS with passport status data.

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 authorize user 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 instance of inaccurate data.

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

- 22 U.S.C. 211a–218, 2651a, 2705
- 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 Procdure)

- 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)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The PIERS system collects the minimum amount of information required to satisfy the statutory purposes of the system and the mission of the bureau. All of the information that is collected by PIERS is required to check the status of issued and expired passports, not issued applications, and destroyed/stolen/lost passports and Consular records of overseas birth and deaths.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

PIERS provides authorized users at both domestic agencies and overseas 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 support 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. Record can be corrected to maintain data integrity. PIERS also support 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.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

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

a. 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.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

None. An individual's information is retained in the system for a time period that does not extend beyond the allotted time specified in the Department of State's Disposition of Schedule, as defined in Chapter 13 Passport Records. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

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 my internally share of 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.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing privacy information internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. To combat the misuse of information by personnel, there are numerous management, operational and technical controls in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to, annual security training, separation of duties, least privilege and personnel screening.

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, examination, and/or other related tax activities;

- National Counterterrorism center t support strategic operational planning and counterterrorism intelligence activities;
- Office of Personnel management OOPM), other federal agencies, or contracted outside entities to support the investigations OPM, other federal agencies, and contactor 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 t whom the record pertains;'
- Foreign government, to permit such government 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.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing privacy information externally and the disclosure of privacy information is generally higher than internal sharing and disclosure. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text), and the use of unsecured connections are also serious threats to external sharing. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with external sharing and disclosure including, but not limited to, formal Memorandums of Agreement/Understandings (MOA/MOU), service level agreements

(SLA) annual security training, separation of duties, least privilege and personnel screening.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

☐ does not constitute a system of records 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?

Before entering information online, the individual is presented with a Privacy Act statement. Acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use, and authority for collection of information submitted is also described in the System of Records Notice titled STATE-26, Passport Systems.

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.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's purpose and uses.

9. Notification and Redress

a. 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 how to inquire about the existence of records about them, how to request access to their records, and how to request an amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport record 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.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

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 authorize user must first sign a user access agreement before they are 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.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.)

11. Technologies

a. 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.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any Information Technology.

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, PIERS was certified and accredited on December 30, 2009. This authority to operate is valid until December 31. 2012.