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: September 2009

(b) Name of system: Electronic Passport Application Form Web Site

(c) System acronym: 2DPPT

(d) IT Asset Baseline (ITAB) number: 897

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

The Electronic Passport Application Form Web Site is an online passport application system that helps collect passport applicant data. The goals of the system are as follows:

1) Reducing the data entry burden at Passport Production Facilities,
2) Establishing consistency in data collection,
3) Improving data integrity,
4) Allowing for the processing and analysis of all application data, and
5) Providing more efficient and effective services.

The system provides online versions of: Form DS-11, Application for U.S. Passport, Form DS-64 Lost or Stolen Passport, Form DS-4085, Application for Additional Visa Pages and Form DS-82, Application for U.S. Passport by Mail.

(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): N/A

(h) Date of previous PIA (if applicable): December 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?

Information processed may include some or all of the following: applicant's name, address, gender, Social Security Number, occupation, and place and date of birth; parents' information, including their place and date of birth; and spousal information, including place and date of birth.

b. How is the information collected?

Information is obtained directly from the passport applicant.

c. Why is the information collected and maintained?

The information collected is the minimum required to meet the business objectives for the issuance of a passport.

d. How will the information be checked for accuracy?

The source (applicant), providing the information is responsible for verifying accuracy. Specific methodologies for verification employed by CA include, among other things, a system maintained as a live feed, allowing the information to be updated/edited and controlled by drop-down lists, input fields are validated for correct format, and required fields are enforced. Moreover, the individual completing the form is required to certify that the information is complete and accurate.

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

- 22 USC Sec. 211a-218 ("The Secretary of State may grant and issue passports, and cause passports to be granted, issued, and verified in foreign countries by diplomatic and consular officers of the United States, and by such other employees of the Department of State who are citizens of the United States as the Secretary of State may designate, and by the chief or other executive officer of the insular possessions of the United States, under such rules as the President shall designate and prescribe for and on behalf of the United States, and no other person shall grant, issue, or verify such passports.")
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports.)

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

The system collects the minimum amount of information required to issue a passport.

There are numerous management, operational, internal, and technical security controls in place to protect the information. These controls include regular security assessments, physical and environmental security, encryption, role-based access control (enforcing least privilege and separation of duties), personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (eg, firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The information is used to determine whether the individual is entitled to a U.S. passport.

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

Data verification checks will be performed as part of the application process; officials at passport agencies review the information for relevance and accuracy. When an individual completes the application, the system will produce a barcode number that contains biographical information. The receiving passport site will use the barcode to retrieve data. The data from this barcode is then stored in a database, thereby eliminating much of the manual data entry.

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

The system does not use any commercial information, publicly available information, or information from other Federal agency databases. All of the information in the system is derived from the passport applicant.

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

The system is owned by DoS, but contractors are involved with the design and development of the system and will be involved with the maintenance of the system. Privacy Act information clauses have been inserted into all statements of work and become part of the signed contract. Each contractor employee is required to attend mandatory briefings that cover the handling of classified and other such information prior to working on the task.

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.

Appropriate use is regulated by automated controls in the system and the inherent & designed system rules of behavior. Instructions on the use of the system are periodically refreshed and re-issued.

5. Retention

a. How long is information retained?

There is no long-term retention of information within the system. Once an individual completes and submits the data/information portion of the passport application process, thus creating the DS-11/82 form, the data/information is deleted from the system. Furthermore, the retention period of information is consistent with established Department of State Policies and Guidelines as documented in the DoS Disposition Schedule, Chapter 13, Passport Records.

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

None. An applicant'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.

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 system does not store any data; therefore, no other internal systems or organizations have access to any data within the system.

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

The system does not interface with any other government system. Its information is not transmitted to any other system. Information is available only to authorized users of the system. Authorized users have roles assigned to them specific to their functional use. Consequently, strong segregation of duties is achieved.

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

Internal sharing occurs only with authorized users, who are cleared government employees or contractors with work-related responsibilities specific to the access and use of the information. No other internal disclosures of the information within the Department of State are made.

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?

The system does not store any data; therefore, no external organizations have access to any data within the system.

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

Information is not shared with any external organizations.

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

None. Information is not shared with any external organizations.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

System of Records Name: Passport Records **Number:** STATE 26

☐ does NOT contain information covered by the Privacy Act.

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

Before completing an online passport application form, 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.

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

Information is given voluntarily by individuals, in order that a passport may be obtained.

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.

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 notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purposes and uses and its applicable legal requirements.

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?

The system 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 Passport Records (State-26), 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 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 purposes and uses and its applicable legal requirements, thus there are no risks associated with notification and redress.

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?

There are only two levels of users for the system: Internet-based end-user passport applicants who are US citizens, and system/web administrators (SAs). Internet-based end-user (applicant) access is only restricted by the end-users' ability to access the Internet and have the appropriate version of an Internet browser that can support 128-bit encryption. Internet-based end-users (applicants) all have the same level of privilege by design, strictly data entry.

System administrator (SA) privileges are based on job function. Managers approve SA access, and privileges are limited to only those required to perform his or her job.

The system audit trails that are automatically generated by the system are regularly analyzed and reviewed to deter and detect unauthorized uses.

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

All SA 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.

No such residual risk is anticipated. Moreover, 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?

The system uses 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 used.

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

The system does not use any technologies that are considered to cause privacy risk.

12. Security

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

The Department of State operates the system 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, 2DPPT was certified and accredited on May 31, 2008. This authority to operate is valid until May 2011.