OPSS
Privacy Impact Assessment

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: June 3, 2011

(b) Name of system: Online Passport Status Service

(c) System acronym: OPSS

(d) IT Asset Baseline (ITAB) number: 898

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

The OPSS initiative permits a U.S. citizen who has applied for a U.S. passport but not yet received it to utilize the internet and a standard browser to check the status of his or her passport application via a link from the http://travel.state.gov website, specifically at https://passportstatus.state.gov.

The OPSS also consists of an OPSS administrative program on the Department's private network that allows the Department users to update the content of OPSS messages sent to passport applicants, revise the content of the public website, and manage reference data element codes and descriptions. Users can also review logs of status record uploads and public website visits, and create summary reports for management.

(f) Reason for performing PIA:

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

(g) Explanation of modification (if applicable): N/A

(h) Date of previous PIA (if applicable): December 23, 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 personally identifiable information (PII) collected and maintained by the system are the U.S. passport applicant's surname, date of birth (DOB), the last four digits of his/her Social Security number (SSN), and e-mail address. The source of the information provided to OPSS is the Travel Document Issuance System (TDIS) repository server, which is in place for the sole purpose of supplying OPSS with passport status data.

The categories of record subjects in OPSS are individuals who:

- Have applied for the issuance, amendment, extension, or renewal of U.S. passport books and passport cards; or
- Were issued U.S. passport books or cards, or had passports amended, extended, renewed, limited, or denied.

b. How is the information collected?

The OPSS system receives passport status information from the Travel Document Issuance System (TDIS) repository server. OPSS pulls the status information from TDIS to the OPSS database in the Demilitarized Zone (DMZ). Once the status information exists in the OPSS DMZ database, U.S. passport applicants can use the public-facing website to inquire about the status of their passport application. The TDIS PIA contains information about how the PII in TDIS is collected.

The OPSS public-facing website requires the applicant to input identifying information (surname, date of birth, and last four digits of SSN) to retrieve the passport status. The information provided by the applicant is used to query the DMZ database for a matching record. If a record exists, the status information of the passport application (i.e. received, working, approved, mailed) is retrieved and returned to the user. No PII is displayed in the message back to the user. The data that OPSS returns to the applicants provides some assurance as to when their passports will be produced and when they are likely to be mailed. OPSS also enables U.S. citizens to submit an email address to receive electronic status updates via email generated from the Department's private network.

c. Why is the information collected and maintained?

Information is collected to allow a U.S. citizen the ability to retrieve the latest status of his/her passport application. The application effectively permits U.S. citizens to have increased access (24 hours/7 days a week/ 365 days a year) to the government as well as enhances the services currently available to citizens by phone at the National Passport Information Center (NPIC). Each element of PII is necessary to ensure that the status of the correct passport application is retrieved.

d. How will the information be checked for accuracy?

OPSS pulls passport application status information from the Travel Document Issuance System (TDIS) repository server; thus, erroneous data/information is cross-referenced with the TDIS data repository which is also owned and operated by the Bureau of Consular Affairs (CA). The TDIS PIA contains information about how PII in TDIS is checked for accuracy.

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

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. 1185 (Travel Control of Citizens)

- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports)
- 22 U.S.C. Sec. 211a-218, 2651a, 2705 (Passport Application and Issuance)
- Executive Order 11295 (Rules Governing the Granting, Issuing, and Verifying of United States Passports, August 5, 1996)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and 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 processing of PII creates the vulnerability that Department of State employees could use the information for purposes other than those required by the Department. The opportunities for the misuse of PII within OPSS pose a moderate risk. OPSS is determined to have a moderate "confidentiality impact level" due to the amount of potential harm that could result to the subject individuals and the Department if the PII in this system was exposed and/or misused. With the collection of passport data, OPSS has high data element sensitivity and high data subject distinguishability. These factors are mitigated through a very specific context of use, in that OPSS uses passport information for specific passport book or card production, and through a statutorily mandated obligation to protect confidentiality. Therefore, the confidentiality impact level is moderate. Misuse may result in emotional distress to individuals whose PII is compromised and administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State.

The Department of State seeks to address these risks by minimizing the transmission of PII to the minimum required to perform the business function required of OPSS. To appropriately safeguard the information, numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). 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. In addition, these controls are subject to rigorous testing, and formal certification and accreditation (C&A). Authority to operate is authorized by the Chief Information Officer (CIO) for the Department. Security controls are reviewed annually, and the system is certified and accredited every three years or sooner if significant changes are made to the existing application.

4. Uses of the Information

a. Describe all uses of the information.

OPSS was developed to allow a U.S. citizen who has applied for a U.S. passport, and who has the capability to access the Internet, the ability to find the status of his/her passport application. The PII is input by the public user to query the OPSS database for a matching record. If only one record matches the PII input by the user, the passport status for that

record will be displayed. These are the only uses of the PII. PII is not displayed in the data that is returned by OPSS to the user.

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

The OPSS administrative application on the Department's private network can be used by Department users to review logs of status record uploads, public website visits, and create summary reports for management. However, the applicant's PII is not included in the reports. The reports only analyze information limited to non-subject-based statistical information, such as the number of passports in a particular status (i.e. received, processing, approved, or mailed) on an aggregate cycle (i.e., monthly, quarterly, yearly, etc.). Furthermore, no new information is derived.

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 except TDIS, as previously discussed.

d. Are contractors involved in the uses of the PII?

OPSS is a government owned system; however, contractors are involved with the design, development and maintenance of the system. Privacy Act clauses have been inserted into all statements of work and have become part of the signed contract. All users are required to pass annual computer security/privacy training, and to sign nondisclosure and rules of behavior agreements.

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.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted.

All users are screened prior to their employment with the Department of State or with their respective agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire; a name check against applicable government agencies; police, credit and fingerprint records; and may include a personal interview if warranted. In addition, before they are given access to the Department network and any CA/CST system, including OPSS, users are required to sign non-disclosure, acceptable use, conflict-of-interest, and rules of behavior agreements. It is mandatory for all Department of State employees and contractors to complete an annual computer cybersecurity 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.

The CA users, system administrators, and database administrators are given security awareness training to enable them to safeguard sensitive but unclassified data (SBU) from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and

external agencies for the proper disposal of paper that is SBU. In addition, there are technical system security controls in place as described in Section 3(f) above.

5. Retention

a. How long is information retained?

There is no long term retention of information within OPSS. The OPSS Aging Service is responsible for deleting the OPSS application status of all records whose status dates have exceeded the corresponding expiration date. This service deletes email addresses after 60 days and the status log tables after 180 days. Once this occurs, the users' surname, DOB, and the last four digits of their SSN will no longer return a passport status since the record will have been deleted from the database.

The information contained in OPSS is retained in other Department databases, specifically TDIS.

The retention time of passport records varies depending upon the specific kind of record. Files of closed cases are retired or destroyed in accordance with the published record disposition schedules of the Department of State and the National Archives and Records Administration (NARA). Some records, such as case files containing passport applications, are retained permanently at NARA.

Disposition procedures are documented at the Department of State, SA-2, Office of Freedom of Information Act, Privacy, and Classification Review, Room 1239, Department of State, 2201 C Street NW, Washington, DC 20520-1239.

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

Record retention bears on privacy risk in two ways. First, the longer the records exist, the greater the risk to unauthorized use or exposure. Second, the longer the records exist, the more likely inaccuracies will develop as a consequence of aging. The privacy risks are mitigated through the controlled access and rules of behavior that govern the Department users of OPSS throughout the lifetime of the data. Accuracy of the data is dependent on the public individuals providing the self-identifying information.

Security protocols within the Department's private network are used to ensure that the data is stored and processed in a secure environment.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with published Department of State record schedules as approved by NARA.

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?

Data regarding U.S. passport application status and applicant email address information is shared between the Travel Document Issuance System (TDIS) and OPSS. Services located

on the OPSS servers control the pull of information from TDIS and is then replicated to the OPSS database in the DMZ. Once the data is available in the DMZ, public users may access their passport status by using their identifying information to query the database for a matching record.

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 by Department policy for the handling and transmission of Sensitive but Unclassified (SBU) information. Access to electronic files is protected by passwords and is under the supervision of the OPSS System Manager. Audit trails track and monitor usage and access. Finally, regularly administered security and privacy training informs authorized users of proper handling procedures.

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

Any sharing of data, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. These vulnerabilities are mitigated by working closely with the internal sharing organizations to develop secure standard operating procedures for using this data.

Access to information is controlled by access controls defined for each system, i.e. application. User training at the application level is delivered annually in accordance with internal Department of State regulations.

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?

No external organizations have access to data within OPSS.

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

Information is not shared with organizations outside of the Department.

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

Since information is not shared with organizations outside of the Department, there are no risks to privacy.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

- Passport Records, State-26

☐ does NOT contain information covered by the Privacy Act.

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

An applicant voluntarily elects to complete the passport application process. The passport application forms, which are outside of the scope of OPSS, indicate theinformation collected, why, for what purpose the information will be routinely used, who the information will be shared with, and the consequences of not providing the data requested and how it is protected.

Before accessing OPSS to check on the status of his/her passport, the applicant is presented with Privacy and Computer Fraud and Abuse Acts Notices and Disclaimers.

This notice provides the Department of State's privacy policy regarding the nature, purpose, use, and sharing of any personally identifiable information (PII) collected via the OPSS website. The Department privacy policy explains the information practices when a public user provides PII, whether collected online or offline, or when a user visits the Department websites online to browse, obtain information, or conduct a transaction.

Users must acknowledge they have read and understood the notice before they are allowed access to the page to check the status of their passport request. Additionally, the SORN mentioned above, State-26, was published to provide notice to the public of the use of their personal information.

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

Using the OPSS website is a voluntary action by a passport applicant. If public users do not want to use their PII to check on the status of their passport online, they may use the alternate method of calling the NPIC.

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 other special uses of the PII contained in OPSS are permitted. Users are advised on the use of their PII collected at the time they apply for a U.S. passport. This process occurs during the first-time passport request or passport renewal request and is outside of the scope of OPSS.

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.

Notice is given to individuals as described in Section 8(a) above. The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the purpose and uses of OPSS.

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 the right of record subjects. Procedures for notification and redress are published in the System of Records Passport Records (STATE-26), and in rules published within 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 within 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, minimal risks are 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 four levels of OPSS users: (1) Internet-based public end-users; (2) OPSS Administrative Users; (3) System Administrators; and (4) Database Administrators.

System Administrators

System Administrators (SA) are responsible for all daily maintenance, establishing access control lists (ACL's), maintaining user accounts and backups. Managers approve SA access, and privileges are limited to only those required for an SA user to perform the specified job. All such authorized users are required to maintain a security clearance level commensurate with their position. To gain authorized access to the Department network and to the system, the employee must pass mandatory cybersecurity and privacy awareness training. System audit trails are automatically generated and are regularly analyzed and reviewed to deter and detect unauthorized uses.

Database Administrators

The database administrators are the only users with direct access to the database for the purpose of performing daily maintenance, upgrades, patches/hotfixes, and database configuration. Database administrators' access is limited to only those Oracle application files necessary to perform daily activities. This limit of access is controlled through the use of access control lists (ACLs) as established by the system administrators. All such authorized users are required to maintain a security clearance level commensurate with their position. To gain authorized access to the Department network and to the database, the employee must pass mandatory cybersecurity and privacy awareness training. Database level auditing is in place and automatically generated at the database level.

Application Administrators (OPSS Administrator)

The OPSS administrative program allows the OPSS administrators to view and maintain information in the OPSS database via the OPSS Administrative Web Site. The application allows authorized users to update the content of OPSS messages sent to passport applicants, revise the content of the public website, and manage the OPSS and TDIS reference data element codes and descriptions. Users can also review logs of status record uploads and public website visits, and create summary reports for management. Enforcement using Windows system authentication will control access to the internal administrative web pages. Access authorizations are controlled by the access level assigned to the user in the OPSS database; application level audit trails are stored in the database.

Public-Internet Users

The OPSS public website is used by U.S. citizens to search for the status of their U.S. passport applications. The U.S. citizen completes the required "identifying information" about the person whose passport application they are requesting status about: last name (i.e. surname), birth date, and last 4 digits of SSN and clicks a "submit" button. If a record matching the required information is found in the OPSS database, a message about the current status of the passport application is displayed. Public internet based users' 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. All internet-based users have the same level of privilege by design.

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

Users internal to the Department must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain access, users must complete annual refresher training.

Internet based users must read and accept the Privacy Act Notice that outlines the expected use of the system.

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 are automatically generated and 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 platform 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.

OPSS does not employ 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 operates OPSS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department has conducted a risk assessment of the system to identify appropriate security controls to protect against risk and implemented controls. The Department performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provisions for the triennial recertification of this system, OPSS completed the Certification and Accreditation (C&A) process, and was granted an Authority to Operate (ATO) that will expire in August 2011. OPSS is currently undergoing a full C&A that will result in a new ATO prior to the current expiration.