

OPSS PIA

1. Contact Information

A/GIS/IPS Director
 Bureau of Administration
 Global Information Services
 Office of Information Programs and Services

2. System Information

- (a) **Name of System:** Online Passport Status Service
- (b) **Bureau:** Bureau of Consular Affairs (CA)
- (c) **System Acronym:** OPSS
- (d) **iMatrix Asset ID Number:** 898
- (e) **Reason for Performing PIA:**
- New System
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization
- (f) **Explanation of modification (if applicable):**

3. General Information

- (a) **Does the system have a completed and submitted Security Categorization Form (SCF)?**
- Yes
- No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.
- (b) **What is the security Assessment and Authorization (A&A) status of the system?**
- The Online Passport Status Service version 03.01.02 was granted an Authorization to Operate (ATO) on July 31, 2013 for 36 months. The current OPSS ATO will expire on July 31, 2016.
- (c) **Describe the purpose of the system:**
- OPSS 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>.

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. OPSS administrative users can also review logs of status record uploads and public website visits, and create summary reports for management.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

OPSS collects 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.

(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)
- 8 U.S.C. 1185 (Travel Control of Citizens)
- 8 U.S.C. 1401–1503 (Acquisition and Loss of U.S. Citizenship or U.S. Nationality)
- 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, 1966)
- 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) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

SORN Name and Number: Passport Records, State-26

SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): Volume 80, Number 56, Tuesday, 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 Division 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 .)

A-13-001-23 Routine Passport Application Status Check and Expedite Fee Upgrades E-mail.

Description: E-mail messages regarding the status of passport applications and requests for expedited service.

Disposition: TEMPORARY: Destroy/delete when 25 days old.

DispAuthNo: N1-059-98-3, item 1

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 Legal Permanent Residents)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes
 No

- If yes, under what authorization?

Yes, it is necessary. OPSS collects only the last four digits of an individual's social security number. OPSS gets this information from its connection with TDIS. The collection of SSNs is authorized under 26 U.S.C. 6039E.

(c) 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. Once the status information exists in the database, U.S. passport applicants can use the public-facing website to inquire about the status of their passport application.

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 OPSS 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 sent 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.

(d) 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.

(e) What process is used to determine if the information is accurate?

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.

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

The data in OPSS is as correct as the public user's input of their personal data into his/her passport application. Then the data flow of the entire Passport suite of applications takes over to verify that the data is legitimate and complete. All of the upstream CA systems for the Passport suite (TDIS, PIERS, PRISM to include archival systems for previously issued passports) are involved in adjudication and production of a passport. These systems come together in multiple layers of interaction for identity verification, including external outreaches to Social Security Administration (SSA) Live and other 'Namecheck' avenues. The passport applications are vetted thoroughly for accuracy. OPSS receives its data through these applications' "handshakes" to show correct data.

(g) Does the system use information from commercial sources? Is the information publicly available?

The system does not use commercial information, publicly available information, or information from other federal agencies.

(h) Is notice provided to the individual prior to the collection of his or her information?

An applicant voluntarily elects to complete the passport application process. The passport application forms, which are outside of the scope of OPSS, indicate the information collected, why, for what purpose the information will be routinely used, with whom the information will be shared, 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. The privacy 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 Passport Records, was published to provide notice to the public of the use of their personal information.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?

Yes

No

If yes, how do individuals grant consent?

Using the OPSS website is voluntary. 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 (National Passport Information Center).

If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?

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 were 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 assessment and authorization (A&A). Authority to operate is authorized by the Chief Information Officer (CIO) for the Department. Security controls are reviewed annually, and the system is assessed and authorized every three years or sooner if significant changes are made to the existing application.

5. Use of the Information

(a) What is/are the intended use(s) for 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) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the system was designed to allow U.S. citizens who apply for US passports to check the status of their application.

(c) Does the system analyze the information stored in it?

- Yes
 No

If yes:

(1) What types of methods are used to analyze the information?

The OPSS administrative application on the Department's private network can be used by Department application administrators to review logs of status record uploads and public website visits, and to 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; for example, the number of passports received, processed, approved, or mailed during a month, quarter or year.

(2) Does the analysis result in new information?

Yes. The results are merely statistics based on usage. For more information refer to 5C(1).

(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

6. Sharing of Information

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

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, which 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.

No external organizations have access to data within OPSS.

(b) What information will be shared?

Data regarding U.S. passport application status and applicant email address information is shared between the TDIS and OPSS.

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

To provide passport applicants with the status of their application.

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

Information is shared by utilizing the State Department secure internal network. The sharing is permitted based on Department policy for the handling and transmission of Sensitive but Unclassified (SBU) information.

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

External Sharing: Information is not shared with organizations outside of the Department of State.

Internal Sharing: Information is shared by secure transmission 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.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Data sharing 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. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

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 Notice for Passport Records (STATE-26), and in regulations published at 22 CFR 171. The procedures inform the individual how to inquire about their records, how to request access, and how to request amendments. 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, and in the interests 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.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes

No

If yes, explain the procedures.

Procedures to allow an individual to correct inaccurate or erroneous information are published in the System of Records Notice for Passport Records (STATE-26), and in regulations published at 22 CFR 171. The procedures inform the individual how to inquire about their records, how to request access, and how to request amendments.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

The procedures are posted on the OPSS web site.

8. Security Controls

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

The OPSS web pages presented to end users on the Internet are protected by 128-bit encryption (https) throughout the user session.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

User access to information is restricted according to job responsibilities and requires managerial level approvals.

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

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information. This is referred to as a multilayered approach. Monitoring occurs from the moment an authorized user attempts to authenticate to the network. From that point on any changes (authorized or not) that occur to data are recorded. If an issue were to arise, administrators of the system would review (audit) the logs that were collected from the time a user logged on till the time they signed off. Ultimately it is very difficult to totally prevent an incident from occurring but by implementing a multilayered approach, risk can be greatly reduced.

(d) Explain the privacy training provided to authorized users of the system.

All Department of State users are required to take annual security awareness training in an effort to safeguard sensitive but unclassified (SBU) data. In addition, any authorized users of OPSS that handle PII are required to take PA459 - Protecting Personally Identifiable Information.

(e) Are any security controls such as encryption, strong authentication procedures, or other controls in place to make the information unusable to unauthorized users?

- Yes
 No

If yes, please explain.

The OPSS web pages presented to end users on the Internet are protected by 128-bit encryption (https) throughout the user session.

(f) How were the security measures above influenced by the type of information collected?

The information collected contains PII and by law must be protected. The measures implemented were the result of considering the amount and type of PII that OPSS collects from the end user.

9. Data Access

(a) Who has access to data in the system?

The following CA personnel have access to the system: System/Web Administrators, Application Administrators and Database Administrators.

(b) How is access to data in the system determined?

Access is role-based according to a need to access by each system user.

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

- Yes
 No

CA/CST adheres to a formal, documented audit and accountability policy that addresses purpose, scope, roles, and responsibilities. In addition, there are documented procedures to facilitate the implementation of the policy and the audit and accountability controls.

(d) Will all users have access to all data in the system or will user access be restricted? Please explain.

There are three types of OPSS user roles: System/Web Administrators, Application Administrators and Database Administrators (DBA). Each of these users will have varying degrees of access to the data based on the roles/job functions that they perform.

(e) What controls are in place to prevent the misuse (i.e. unauthorized browsing) of data by users having access to the data?

There are various management, operational, and technical controls in place and these controls are tested annually to validate they are in place and working as expected. As an example all accounts are subject to automatic auditing. Audit logs are reviewed at the Application, Database, and System level as follows:

Application level: OPSS administrators review the application level audit logs as necessary and take the appropriate action if suspicious activity or suspected violations are identified.

Database level: System Services and Operations (SSO) reviews the Structured Query Language (SQL) logs for indications of inappropriate or unusual activity on the OPSS database, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

System level: SSO reviews the Operating System (OS) logs for indications of inappropriate or unusual activity on the OPSS system, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.