PRIVACY IMPACT ASSESSMENT

Online Passport Status Service (OPSS)

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) **Name of system:** Online Passport Status Service

(b) **Bureau:** Consular Affairs (CA)

(c) **System acronym:** OPSS

(d) **iMatrix Asset ID Number:** 898

(e) **Reason for performing PIA:**

☐ New system – Logical Consolidated Boundary

☐ 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 system is currently undergoing its Assessment and Authorization (A&A) in order to receivan Authorization to Operate (ATO) status. OPSS is expected to receive its ATO by Winter 2020.

(c) Describe the purpose of the system:

OPSS supports the Bureau of Consular Affairs' mission requirements to permit U.S. citizens who have applied for a passport but not yet received it to utilize the Internet and a standard browser to check the status of the passport application via a link from the travel.state.gov website. The OPSS application provides U.S. citizens with quick and easy 24 hour access to their application status. As a result, the National Passport Information Center (NPIC) resources are more available to address questions that require specialized knowledge. The OPSS system requests identifying information from the applicant, retrieves the latest status of the passport application (i.e., received, working, approved, mailed) and provides this information to the applicant. The OPSS system receives status information from the Travel Document Issuance System (TDIS) repository server. The OPSS provides information on when an applicant's passport will be produced and a tentative date it will be mailed. OPSS also enables U.S. citizens to submit an email address to receive electronic status updates via email generated from the OPSS.

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

U.S. Citizen: name, birthdate, Social Security Number (SSN) (OPSS collects only the last four digits of the SSN), phone number, home address, and email address.

(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 Documentation of Aliens and Citizens)
- 8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 22 U.S.C. Sec. 211a-218, 2651a, (Passport Application and Issuance)
- 22 U.S.C. 3927 (Chief of Mission)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- Executive Order 11295, August 5, 1966; (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

STATE-26, Passport Records, March 24, 2015
STATE-05, Overseas Citizens Services Records and Other Overseas Records, September 8, 2016

☐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 .)

Schedule number Department of State Records Disposition Schedule:

A-13-001-23 - Routine Passport Application Status Check and Expedite Fee Upgrades E-mail
Description: Email messages regarding the status of passport applications and requests for expedited service.
Disposition Temporary: Destroy/delete when 25 days old
DispAuthNo: N1-059-98-03, item 1

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system?

☒ Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)

☒ U.S. Government/Federal employees or Contractor employees

☐ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

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

☒Yes ☐No

Yes, it is necessary. OPSS collects only the last four digits of an individual's social security number. OPSS gets this social security information from its connection with TDIS. When applicants log into OPSS to request the status of their passport, they must input the last four digits of their Social Security number for verification, however it is originally obtained in the system from TDIS.

- If yes, under what authorization?

Executive Order 9397, November 22, 1943; Executive Order 13478, November 18, 2008.
26 U.S.C. 6039E - Information Concerning Resident Status
22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(c) How is the information collected?

OPSS receives information from another DoS IT system. Passport status information is gathered by OPSS from the Travel Document Issuance System (TDIS) repository server. OPSS pulls the status information from TDIS to the OPSS database.

The passport applicant does not submit information diretly to OPSS, however once the status information exists in the OPSS 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 listed on paragraph 3(d), to retrieve the passport status. This information is already in the OPSS system by the time the applicant enters it into the public facing website.

(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 CA. After submission of applications, CA passport applications (TDIS, Passport Records Imaging Systems Management (PRISM) and Tracking Responses and Inquiries for Passports (TRIP) verify that the data is legitimate and complete. 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.

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

The applicants are responsible for ensuring that the information is current when they request the status of their passport application via OPSS. Information is also checked via other CA systems discussed in paragraph 4e for currency.

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

No, OPSS does not use commercial or publicly available information.

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

Ye**s,** a Privacy Act Statement (PAS) is prominently displayed on the OPSS webpage that collects the PII.

(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?

The applicant is advised of all relevant privacy implications via a Privacy Act Statement at the source of collecting the information via the OPSS system. The OPSS website provides an Opt In checkbox where the applicant reads the Privacy Act Statement and must check the box agreeing to it before being allowed to continue.

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

The OPSS PII listed in Question 3d is the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered and addressed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the OPSS system to perform the function of providing the applicants the status of their passport applications.

5. Use of information

(a) What is/are the intended use(s) for the information?

The PII in OPSS is used to allow a U.S. citizen who has applied for a U.S. passport to check the status of his/her passport application via the internet. The PII is entered by the public user to query the OPSS database for a matching record. If the OPSS record matches the PII entered by the user, the passport status for that record will be displayed.

(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 PII required allows U.S. citizens who apply for US passports to check the status of their application via the OPSS system.

(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**?

OPSS provides automated statistical workflow reports that do not include any PII.

(2) Does the analysis result in new information?

☒Yes

Only the statistical data is new, which does not include PII.

☐No -

(3) Will the new information be placed in the individual's record?

☐Yes

☒No Only statistical data, which does not include PII, is used to track passport application status only.

(4) With the new information, will the State 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.

Only authorized Department of State employees, and cleared contractors within CA who have a justified need for the information in order to perform official duties have access to OPSS data.

OPSS does not share information internally or externally. External organizations do not have access to data within OPSS.

(b) What information will be shared?

OPSS does not share information internally or externally. External organizations do not have access to data within OPSS.

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

OPSS does not share information internally or externally. External organizations do not have access to data within OPSS.

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

OPSS does not share information internally or externally. External organizations do not have access to data within OPSS.

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

The OPSS system does not share information internally or externally. External organizations do not have access to data within OPSS.

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

The OPSS system does not share information internally or externally. External organizations do not have access to data within OPSS.

7. Redress and Notification

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

All applicants can follow instructions for gaining access as stated in System of Records Notices (SORNs) State-26 (Passport Records) and State-05 (Overseas Citizens Services Records and Other Overseas Records). They may also visit the Department of State public site and/or the Department of State Privacy Act/FOIA web site for the privacy policy which includes instructions on how to obtain access by contacting the listed offices by phone or by mail.

In addition, applicants can access information in the OPSS system. The OPSS system is used only to track passport status. Applicants can access the OPSS website, input requested information and can view the information it contains on the status of their passport application.

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

☒Yes ☐No

If yes, explain the procedures.

Applicants can follow instructions for requesting changes to their information as stated in SORNs STATE-26 (Passport Records) and STATE-05 (Overseas Citizens Services Records and Other Overseas Records). They may also visit the Department of State public site and/or the

Department of State Privacy Act/FOIA web site for the Privacy Policy which includes instructions on how to request changes by contacting the listed offices by phone or by mail.

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

The Privacy Act Statement is located at the point of collection of information. It lists SORNS STATE-26 and STATE-05 that provide procedures to correct information. Additionally, telephone help numbers are posted on the Passport Status Check site where information is collected to address concerns the applicant may have, including how to correct their information. Information on how to amend records and who/what office to get in touch with as well as providing contact information is made available with each of the processes listed above.

If no, explain why not.

8. Security Controls

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

The system is secured within the Department of State intranet where risk factors are mitigated through the use of defense in-depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform their official duties.

Access to OPSS applications/databases is further protected with additional access controls set at the application/database level. All system accounts/access must be approved by the user's supervisor and the Information System Security Officer (ISSO). The audit vault system is used to monitor all privileged access to the system and violations are reported to senior management daily, if applicable.

Applications are configured according to the Department of State Bureau of Diplomatic Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST 800-53) and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program.

(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.**

To access the system, persons must be authorized users of the Department of State's unclassified network which requires a background investigation and an application approved by the supervisor and ISSO. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the OPSS system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports to be restricted. Security officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(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. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name

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

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component to accss or use systems. Additionally, Department of State civilian employees are required to take the one-time course (PA459 Protecting Personally Identifiable Information). The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(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.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Bureau of Diplomatic Security, Security Configuration Guides to reduce and mitigate the risks associated with internal transfers. Data in transit from TDIS to OPSS is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) How were the security measures above influenced by the type of information collected?
Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above were implemented to secure the data in the system in accordance with federal laws and policies, including Department policies.

9. Data Access

(a) **Who has access to data in the system?**
Public Users, Department of State approved OpenNet-based Users, System Administrators, and Database Administrators.

(b) **How is access to data in the system determined?**
Access is determined based on role-based requests which are approved by the supervisor and the ISSO. Access is role based and the user is granted only the role(s) required to perform official assigned duties.

(c) **Are procedures, controls or responsibilities regarding access to data in the system documented?** ☒Yes ☐No
Information is documented in the System Security Plan. The Plan includes information regarding system access to data.

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

There are four types of OPSS user roles: Public users, OPSS OpenNet Users (Department of State employees and contractors), System Administrators, and Database Administrators.
Users other than administrators do not have access to all data in the system. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

Public Users – The public only has access to their information in the OPSS system. Required PII outlined in paragraph 3d must be entered to acquire access to the applicant's information to check the status of the applicant's passport.

DoS OPSS Users- Access to OPSS is restricted to cleared Department of State direct hire and contractor employees. Department of State employees and contractor are assigned access privileges based on their job functions. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

System Administrators - The System Service and Operations Project Manager completes the CA/CST online System Administrator Account Request Form. OPSS Administrators are authorized to access the system for the purpose of performing daily maintenance, establishing access control lists, troubleshooting technical issues and installing software. The Project Manager reviews the role and approves the form authorizing the account to be established and activated. OPSS System Administrators have logon identifications associated with their name that allows for user auditing.

Database Administrators – OPSS Database Administrators (DBA) are responsible for the daily maintenance, upgrades; patch/hot fix application, backups and configurations to the database. DBA access is controlled by the Integrated Services (IS) team through the use of access control lists (ACLs) as established by the system administrators.

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

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented; access is role based as required by policy.

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN)

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing.