PRIVACY IMPACT ASSESSMENT

Online Passport Renewal (OPR)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: March 24, 2021

(b) Name of system: Online Passport Renewal

(c) System acronym: OPR

(d) Bureau: Consular Affairs

(e) iMatrix Asset ID Number: 184958

(f) Child systems (if applicable) iMatrix Asset ID Number: N/A

(g) Reason for performing PIA:

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

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

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?

☒ Yes
☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?

☒ Yes
☐ No

If yes, has the privacy questionnaire in Xacta been completed?
☒ Yes
☐ No

(c) Describe the purpose of the system:

The ConsularOne (C1) program is intended to modernize and consolidate the existing operational environment under a common technology platform in order to better support the services provided to CA's customers. CA expects the software elements of the solution architecture to be the major components of the common technology platform for ConsularOne. The OPR system is one of the business applications in the C1 environment.

The purpose of the ConsularOne Online Passport Renewal (OPR) system is to provide the capability for U.S. Citizens to apply for passport book/card renewals online. The OPR system will have a positive impact towards streamlining what is currently a paper-intensive process. It provides Consular Affairs (CA) with enhanced capabilities to respond to surges in passport demands and enable the Department of State to adjudicate and deliver quicker streamlined customer service for passport book/card renewals.

The OPR system will also provide enhanced services such as Photo Quality Check services, paperless data and fee submissions with electronic signature, status updates online, and email notifications to the applicant. The OPR system will use external service providers, United States Postal Service (USPS), Pay.gov, Social Security Live (SSL) and LexisNexis in processing passport service requests.

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

The system will contain name, birthdate, place of birth, phone number, email address, personal mailing address, last known permanent address, alternate names, social security number (SSN), family information, gender, age, biometrics, photograph, passport book/card information, height, hair and eye color.

(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)
- 22 U.S.C. Sec. 211a-218, 2651a, 2705 (Passport Application and Issuance)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- 22 U.S.C. 3927 (Chief of Mission)
- 26 U.S.C. 6039E (Information Concerning Resident Status)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)

☒ Yes, provide:

- SORN Name and Number: STATE-26, Passport Records,
- SORN publication date: March 24, 2015

- SORN Name and Number: STATE-05, Overseas Citizens Services Records and Other Overseas Records
- SORN publication date: 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 Office 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 A-records@state.gov.)

If yes provide (Consolidate as much as possible):

- **Schedule Number:** A-13-002-02 - Requests for Passports
- **Disposition Authority Number**: N1-059-05-11, item 2D
- **Length of time the information is retained in the system**: Temporary: Cut off at end of calendar year. Hold in current file area and retire to Records Service Center when 2 years old. Destroy/delete when twenty-five (25) years old.
- **Type of information retained in the system:**
  Application data/applicant photo and adjudication data for online passport book/card renewals are retained in the system with the exceptions of purged data noted above**.**

- **Schedule Number:** A-13-001-23 - Routine Passport Application Status Check and Expedite Fee Upgrades E-mail
- **Disposition Authority Number:** N1-059-98-03, item 1
- **Length of time the information is retained in the system:** Destroy/delete when 25 days old.
- **Type of information retained in the system:** Email messages regarding the status of passport applications and requests for expedited service.

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 LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒ Yes ☐ No ☐ N/A

- If yes, under what authorization?
26 U.S.C. 6039E - Information Concerning Resident Status; and
22 U.S.C. § 2714a.(f) Revocation or Denial of Passport in Case of Individual without Social Security Number

(d) How is the PII collected?

The OPR system receives information directly from the applicant via the public-facing site for online passport renewals. Applicants use their MyTravel.State.Gov account on the public-facing Travel.State.Gov website to request the OPR service to apply for passport book/card renewals.

(e) 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.

(f) What process is used to determine if the PII is accurate?

Information provided is checked against the information retrieved from the interfacing systems listed in section 6(a) for accuracy. The OPR system compares the applicant's historical passport book/card data with the applicant-provided PII for any discrepancies. Information is also verified for accuracy via the United States Postal Service; the Social Security Administration, and LexisNexis.

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

The applicant is responsible for ensuring that the information provided is current for the renewal of passports. Applicants are required to sign the application stating that the information provided is current upon submission. Additionally, information is also checked for discrepancies which can relate to the applicant's current status in a number of ways during the processing of the passport book/card renewal application as stated in paragraph 6(a) via other CA systems, federal agencies and LexisNexis.

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

Yes, information is used from LexisNexis to assist in verifying a passport renewal requester's information by detecting errors or fraudulent information. The LexisNexis information is publicly available.

(i) How was the minimization of PII in the system considered?

An assessment of required PII was performed to determine what information is required to effectively implement the online passport renewals. The PII listed in paragraph 3(d) is the minimum required to conduct online passport renewals. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the OPR system to perform the functions for which it is intended, which is to process passport renewals.

5. Use of information

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

The required PII is to be used to validate the applicants' eligibility of passport renewals and the processing of the online passport renewal requests.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the PII is used to validate the applicant's eligibility, to process online passport renewal requests, to correspond with the applicant, and to provide status updates.

(c) Does the system analyze the PII stored in it? ☒Yes ☐No

If yes:

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

The OPR system compares the applicant's historical passport book/card data with the applicant-provided PII via other CA Systems listed in paragraph 6a. The OPR system also compares the SSN provided by the applicant with the results from SSA Live or LexisNexis if SSA Live is not available.

(2) Does the analysis result in new information?

Yes, the data generated by the OPR system from the other source systems provide passport adjudicators new information such as evidence of fraud, owing of federal taxes, legal issues, or criminal activity. Depending on the situation, the resulting information may lead to denial of passport renewal.

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

The new information will be stored with the specific case/application that has been adjudicated.

(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

(d) If the system will use test data, will it include real PII? ☐ Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal: The term "internal sharing" traditionally refers to the sharing of information with the Department of State (DoS), but external to the owning organization (referred to as "bureau" at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau. With that understanding, information in the OPR system is shared internally with other CA systems as follows: Consular Consolidated Database (CCD); ConsularOne Applications and Data (CAD); ConsularOne Data Infrastructure (CDI); ConsularOne Platform and Infrastructure (CPI); Enterprise Payment System (EPS); Travel Document Issuance System (TDIS); Management Information System (MIS); Passport Information Electronic Records System (PIERS) and its associated databases such as the Vital Passport Records Repository (VIPRR) database; Consular Lookout and Support System (CLASS) and its component, Consular Lost and Stolen Passports (CLASP); Passport Lookout Tracking System (PLOTS); Enterprise Payment System (EPS); and the Passport Records Imaging System Management (PRISM).

External: OPR PII is shared externally with the United States Postal Service, the Social Security Administration (SSA), LexisNexis, and Pay.Gov.

(b) What information will be shared?

Internal: The information in paragraph 3(d) will be shared for passport book and card renewal requests with the CA systems addressed in paragraph 6(a).

External: The following will be shared with external entities:

- United States Postal Service - mailing address
- Social Security Administration - applicant's name, alternate name(s), social security number, date of birth
- LexisNexis - name, SSN, date of birth, place of birth, telephone number, and permanent address
- Pay.gov - name, mailing address, amount due.

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

Internal: Information is shared internally to assist in verifying the applicant's information, to conduct eligibility status checks, to adjudicate and process passport book/card renewals, and to correspond with the applicant and provide status updates.

External: Information shared with the United States Postal Service is used to obtain the complete zip +4 mailing address in order to mail the passport book/card to the applicant. Information shared with the Social Security Administration is used to validate the Social Security Number of the applicant as part of the adjudication process for a passport book/card renewal. Information shared with LexisNexis is used to assist in detecting errors or fraudulent information. Information shared with Pay.Gov is used to process payments for the passport services requested by U.S. citizens.

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

Internal: The internal CA systems listed in paragraph 6(a) share information via the State Department secure internal network (OpenNet). The sharing is permitted based on State Department policy and approved protocols for the handling and transmission of sensitive but unclassified (SBU) information. Systems share information via database to database via Hypertext Transfer Protocol Secure (HTTPS) transmission. HTTPS is used to secure encrypted communications over the internet using Transport Layer Security. The connection between all the CA sites that the system servers reside is protected using HTTPS.

External: US Postal Services information is transmitted via HTTPS. SSALive Services provides interconnection with SSA is via HTTPS. LexisNexis is accessed by the OPR system via service-oriented architecture (SOA) services which are in the ConsularOne Platform and Infrastructure (CPI) SOA services zone. Information transmitted via the ConsularOne CPI is via Hypertext Transfer Protocol Secure (HTTPS). OPR submits requests via CPI to EPS for pay.gov payment services. Information among the CA systems OPR, CPI and EPS is transmitted via HTTPS.

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

Internal: Information is shared by secure transmission methods (HTTPS) permitted by internal Department of State policy for the handling and transmission of Sensitive but Unclassified (SBU) information. Internally, the information is accessible to only authorized OPR system users and is subject to stringent access policies, auditing and monitoring. All accounts are approved by supervisors and the local System Security Officers. Audit trails track and monitor usage and access. In accordance with U.S. government policies, any federal government employee or contractor with access to Personally Identifiable Information (PII) must adhere to strict requirements for protection and storage of PII. Department of State personnel are required to comply with these requirements and to complete yearly and biennial training regarding cyber security and the protection of PII. Additionally, passport personnel are also required to take yearly passport specific training, which informs authorized users of proper handling procedures regarding access and use of PII in passport systems.

External: Memorandums of Understanding/Interagency Service Agreements are in place with the US Postal Service, the Social Security Administration and the Department of Treasury regarding pay.gov for the use and handling of information. A service agreement is in place with Lexis Nexis to retrieve the OPR query results. HTTPS is used to secure encrypted communications over the internet using Transport Layer Security for external communication.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes, notice is provided to the applicant prior to collection of information. A Privacy Act statement is provided that the applicant must acknowledge reading by clicking on the button to allow them to complete the online passport renewal request.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒Yes ☐No

If yes, how do record subjects grant consent?

Applicants grant consent by clicking on the button acknowledging that they have read the Privacy Act statement which states if requested information is not provided it may result in denial of an application or delay in processing.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

Applicants cannot gain access to information once the application is submitted. However, prior to submission applicants can review and edit all data. Also, applicants can download and print the application data they entered into the OPR system's public-facing application form. In addition, applicants can follow the procedures for accessing information outlined in the published SORNs, STATE-26 and STATE-05, or the Department of State Privacy Policy link on the Department of State website.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Prior to submission, applicants are presented with a "Final Review" screen, which provides all information entered, as well as a link to each section of the application, should the applicant wish to make changes. The applicant must also check a box to indicate that the application data are true and correct. Thereafter (upon successful submission and while the application is being processed) applicants can update the mailing address and contact information if necessary by opening a service request via the

OPR system. Once the application is submitted, applicants do not have access to the information in the OPR system. However, procedures are outlined in the published SORNs, STATE-26 and STATE-05, on processes to amend information.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

Procedures are outlined in the published SORNs, STATE-26 and STATE-05, on how to correct information in records. Also, once information is submitted, applicants are notified by email of any correspondence that awaits them in the OPR public-facing application requiring correction and the procedures**.**

8. Security Controls

(a) **How is all of the information in the system secured?** The OPR system is secured within the Department of State internal network (OpenNet), 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 OPR is further protected with additional access controls set at the database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer (ISSO). The audit vault system is used to monitor all privileged access to the system. Audit trails are reviewed daily for suspicious activities, which are required to be reported to senior management immediately. OPR is configured according the State Department 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) **Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).**Access to the OPR system is role-based and the user is granted only the roles(s) required to perform officially assigned duties. There are five types of users: Public Users, OPR Siebel Administrators, Database Administrators, Passport System Administrators, and Internal OPR Passport Users.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

External accounts are managed via the CA CAD Customer Account Management (CAM) Portal. Anyone in the world can logon to Travel.State.GOV (TSG) and request a MyTravel.State.Gov account via the CAM Portal. There is no account approval process to request a MyTravel.State.Gov account via CAM Portal. Through the MyTravel.State.Gov account, the applicant can request citizen OPR services. Citizens can only see their information in the OPR system when entering data. Once data are submitted, the applicant can no longer see the information.

Internal Department of State users are provided access based on their job functions approved by their supervisor and the local Information System Security Officer. Access is controlled by the Access Control Lists implemented within the OPR system.

(d) How is access to data in the system determined for each role identified above?

Access is role-based and restricted according to approved job responsibilities and requires managerial concurrence. Each authorized OPR system user must be approved by the supervisor and sign the user access agreement/rules of behavior before being given an OpenNet user account and access to the OPR system. Access is role-based. Access control lists, based on the approved job responsibilities permit categories of information to be accessed by individuals. Information System Security officers (ISSO) 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.

Public Users: Public users are able to create a MyTravel.Gov online account to access the OPR system. Public users can only access the OPR system to renew their passport book/card online. Public users can only see and access their PII prior to their submission. Prior to submitting, the applicant is required to check a box stating that the application is true and correct.

Siebel Administrators: The Siebel administrators include both government employees and contractors. Siebel administrators are responsible for all daily maintenance, establishing access control lists (ACLs), and backups. Siebel administrators can see and access OPR system information. The process for a Siebel administrator to request privileged access is to create a ticket via the Remedy system, and the ticket is reviewed/approved by the administrator's supervisor, the Government Technical Monitor (GTM), and the ISSO.

Database Administrators: Database administrators (DBA) are responsible for the maintenance, upgrades, patches/hotfixes, and database configuration. The access of database administrators is limited to only those database application files necessary to perform daily activities. The DBA has access to information in the OPR system, but can only perform assigned functions. DBA access is controlled through Access Control Lists (ACLs), as established by the system administrators. The process for a DBA to request privileged DBA access is to create a ticket via the Remedy system, and the ticket is reviewed/approved by the DBA's supervisor and the GTM and the ISSO.

Passport (PPT) System Administrator: Passport (PPT) system administrators provide system and application administration support for local Passport Centers throughout the country. The system administrator can see and has access to information in the OPR system. The local ISSO is responsible for reviewing and approving system administrator accounts.

Internal DoS Passport Users: Following are the Internal DoS Passport user responsibilities and the related access, as approved by supervisors:

- PPT Adjudicators: Access to case summaries and searches in the OPR system**.**
- PPT Agency Director & PPT Assistant Director: Access to information to support management activities. Can access all OPR information.
- PPT Image Supervisor, PPT Image Reviewer and PPT Image Editor: Access to the image worldwide case queue, which contains the photo gallery.
- PPT Communications Supervisor and PPT Communications Clerk: Access to assigned cases, some case queues and some service tasks.
- PPT Passport Service Associate: Can view and edit the contents of service requests (passport renewals) submitted by customers.
- PPT Site Administrator: Ability to view the number of passport applications in progress and a report of exception cases.
- PPT Executive: Access to case search tasks, site administration tasks. The PPT Executive can access all information in OPR.
- PPT Legal Reviewer: Access to the case summary for Legal CLASS lookouts, reference data checks and notes, and the passport headquarters legal queue. The legal reviewer has access to all OPR information.
- PPT Fraud Reviewer: Access to the fraud case queue. The Fraud Reviewer has access to all the information in OPR.
- PPT HQ Adjudication Reviewer: Access to the case summary notes and the passport headquarters adjudication queue. The PPT HQ Adjudicator has access to all the Fraud Case information in OPR.
- PPT HQ Fee Issue Reviewer: Access to the pre-adjudication issues worldwide case queue. The fee issue reviewer has access to all the information in OPR.
- PPT National Customer Service: Limited access to OPR information in the search functionality in support of call center tasks.
- PPT Business Administrator: Access to OPR administrable information.

(e) What monitoring, recording, auditing safeguards, and other controls 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 (PII). At the case/application level data changes are recorded in the case trace. At the system-wide level a query log that includes date/time, query criteria and the person querying is maintained and searchable. In accordance with Department of State Security Configuration Guides, OPR auditing is also enabled to track the following events on the OPR host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the OPR audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

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

☒Yes ☐No

Procedures are addressed in the OPR System Security Plan regarding access to data in the system.

(f) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

The following various required privacy training is required for individuals accessing OPR:

In accordance with Department of State computer security policies, mandatory annual security training (PS800 Cyber Security Awareness) is required for all authorized users of OPR. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component.

PA318 Protecting Personally Identifiable Information is a mandatory biennial course required for all DoS personnel and contractors accessing DoS computers.

The Passport Services Internal Control Guide requires all passport personnel (government and contractors) to complete the Passport Data Security Awareness (PC441) course as an annual recertification to maintain access to OPR. This course provides refresher training on the Privacy Act, Personally Identifiable Information (PII) and proper handling of PII.