EPA United States
Environmental Protection
Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Passport Expiration Notification System	**System Owner: Sergio Schwimmer**
Preparer: Pamela Younger	**Office: Office of International and Tribal Affairs**
Date: 07/14/2020	**Phone: 202-564-6631**

Reason for Submittal: New PIA____   Revised PIA_Annual Review__X__ Rescindment ____

This system is in the following life cycle stage(s):

Definition ☐ Development/Acquisition ☐ Implementation ☒

Operation & Maintenance ☒ Rescindment/Decommissioned ☐

Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

Provide a general description/overview and purpose of the system:

The purpose of the Passport Expiration Notification system is to track the status of official passports, including the passport number, issuance and expiration dates, and the current location.

The information is used to request and obtain country clearances for EPA staff traveling to foreign countries to conduct official government business.

 To obtain an official passport, each passport holder is required to complete a passport application electronically from the Dept. of State website, and print-out and submit to OITA's International Travel

Office for the Travel Office to submit to the Dept. of State.   The information in PENS is entered into the system only after Dept. of State has issued an official passport. State's review for accuracy and completeness of data serves to mitigate risk.

Section 1.0 Authorities and Other Requirements

1.1   What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

Executive Order 11295--Rules governing the granting, issuing, and verifying of United States passports

Source: The provisions of Executive Order 11295 of Aug. 5, 1966, appear at 31 FR 10603, 3 CFR, 1966-1970 Comp., p. 570, unless otherwise noted.

1.2   Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

PENs is a document library on SharePoint. SharePoint is part of Office 365 solution. Office 365 / My Workplace has a completed Enterprise System Security Plan (SSP) and is currently operating under an Enterprise Services ATO that expires July 12, 2020. OMS/OITO is currently working on a new ATO under ECS - "Email and Collaboration Solutions" which is expected to be submitted in a few months.

1.3   If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

U. S. Department of State Passport Applications (DS-82; DS-11).

1.4   Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes, the data is maintained in a Cloud. The Service is FedRamped approved and the type of service is SaaS.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well

as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

Passport holder's name, state of birth, passport number and passport issue and expiration dates.

2.2 What are the sources of the information and how is the information collected for the system?

State Department issued passport. Passport information is entered into the PENS.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

Applicants for Official Passports complete an on-line form maintained by the Department of State. State reviews the information provided on the form for accuracy and completeness before issuing the Official Passport, which serves as the basis for the data in PENS. In addition to State's review, staff in OITA's the International Travel Office staff regularly review the data in PENS to ensure accuracy.

2.5 <u>Privacy Impact Analysis</u>: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

To obtain an official passport, each passport holder is required to complete a passport application electronically from the Dept. of State website, and print-out and submit to OITA's International Travel Office for the Travel Office to submit to the Dept. of State. The information in PENS is entered into the system only after Dept. of State has issued an official passport. State's review for accuracy and completeness of data serves to mitigate risk.

<u>Privacy Risk</u>:

Low risk of entering inaccurate data into the system.

<u>Mitigation</u>:

The Dept. of State has a review process, as referenced above, which serves to mitigate risk.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

PENS is a platform in Sharepoint. Access to the controls is role-based. The IMO and EPA's passport agents, which must be certified by the Department of State, have full access to the system. Currently, no other employees have been granted system access. Any requests for access would require a justification and must be reviewed and approved by OITA's Senior Information Officer.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Requirements for access to the system are documented in the SOP for PENS.

3.3 Are there other components with assigned roles and responsibilities within the system?

No

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Only certified Passport Agents in the OITA Travel Office, Region 5, and the OITA Database Administrator will have access to the information contained in the database. Contractors do not have access to the system.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Official passport information is retained for up to 3 years after expiration. Official passports are valid for 5 years.

The information is used to request and obtain country clearances for EPA staff traveling to foreign countries to conduct official government business.

Records Control Schedules 0090 and 1010.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

When a passport holder retires or resigns from the agency, they must notify OITA's

International Travel Office, as required by the agency's separation process. The physical passport is returned to the International Travel Office for cancellation and destruction and the information in PENS is permanently deleted. Records are not maintained in PENS past the applicable records retention date.

Passports are returned to the Passport Office for cancellation and destruction once a passport holder has separated from the agency and deleted from PENS.

Privacy Risk:

Low risk of maintain record longer then needed.

Mitigation:

The agency's separation process requires staff who are retiring or separating from service to notify OITA and secure confirmation that their official passport, if one exists, has been turned in to OITA.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Yes. Information from a traveler's Official Passport is shared with the Dept. of State, which issued the Official Passport and already has the information in their internal system. The information is shared for the purpose of requesting country clearances and visas for International Travel.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

The information is not shared externally.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

Not applicable.

4.4 Does the agreement place limitations on re-dissemination?

Not applicable.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated? Not applicable.

Privacy Risk:

None, information is not externally shared

Mitigation:

None

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?
The system is used for the collection of the traveler's name and passport number, which OITA can use to request and obtain country clearances for EPA staff traveling outside of the United States to conduct official government business. The International Travel Office is able to run reports from a separate system, the Fast International Approval of Travel (FIAT) database. FIAT allows the International Travel Office to run reports on demand and to track how many travellers have traveled on their official passports.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.
Users take the annual Information Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of inaccurate or untimely audit

Mitigation:

An accurate and time audit process is in place to ensure all PII are accounted for in the system.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

To request and obtain country clearances for EPA staff traveling to foreign countries to conduct official government business.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X__ No___. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)*

Information is retrieved by passport holder's name.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The OITA Travel Office is evaluated by the Department of State every two years. As part of the evaluation, DOS ensures that there is limited access to only 3 people and that the physical passports are secured in a locked cabinet behind a locked door.

6.4 <u>Privacy Impact Analysis</u>: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.
The system is a SharePoint document library containing information copied from physical passports stored and managed by the International Travel Office and Passport Liaisons There is no automation or data-sharing functionality in the system. Only authorized users will refer to information in the system when working with the Department of State's clearance system.

<u>Privacy Risk</u>:

Low risk of information misuse

<u>Mitigation</u>:

The biennial reviews performed by the Department of State and the limits on access to PENS provide controls]. Controls are in place to ensure the information is not misused.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The notice of collection is stated on the Dept. of State application for an Official Passport. OITA relies on the form to provide notice to individuals. All information in PENS is drawn from Official Passports.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

EPA employees are aware that their passport information is used for the purpose of obtaining country clearances, and visas for International Travel when they request to obtain an official passport.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Individuals may not read the privacy notice or understand the need for the notice.

Mitigation:

Clear notice has been provided by the Department of State provides on the passport application form.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking to obtain information in this system would contact OITA's International Travel Coordinator and International Travel Liaison either by phone, or email and provide their first and last name.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

To request a correction, employees must complete and submit the DS-5504 application and submit to OITA's International Travel Coordinator/Passport Acceptance Agent for submission to the Department of State's Special Issuance Agency.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

None. Appropriate procedures area in place to redress the

Mitigation:

None