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 Roster.docx

| | | | |
|---|---|---|---|
| **System Name: Passport Expiration Notification System (PENS)** | | **System Owner: Sergio Schwimmer** | |
| **Preparer: Sergio Schwimmer** | | **Office: Office of International and Tribal Affairs** | |
| **Date: 3/22/2024** | | **Phone: N/A** | |
| **Reason for Submittal:** | | | |
| New: ☐ | Revised:☒ | Annual Review: ☐ | Rescindment: ☐ |
| **System Lifecycle Stage(s):** | | | |
| Definition: ☐ | Development/Acquisition: ☐ | Implementation: ☒ | |
| Operation & Maintenance: ☐ | Rescindment/Decommission: ☐ | | |

**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:

To identify international and tribal country environmental issues, the Environmental Protection Agency (EPA) created the Office of International and Tribal Affairs (OITA) to help implement policy options to address those issues.

Furthermore, for EPA staff traveling abroad to work on international environmental issues, EPA OITA developed the Passport Expiration Notification System (PENS) to track and manage EPA staffs' country

clearances information. For example, PENS track the status of Department of State (DOS) passport applications, official passports, passport numbers, issuance and expiration dates, place of birth and the current location of the official passports.

The OITA/Office of Management and International Services (OMIS) supports the Agency's international travel efforts and manages PENS. The Travel Office enters the information (Name, Number, Issuance and Expiration Date, and place of birth) into PENS, records the location of the passport (OITA Safe, with the traveler, with the traveler's office, in transit, at a Foreign Embassy for visa processing, or Sent to the Department of State for renewal or disposal), and informs the traveler of the completion. OITA/OMIS staff use this data when requesting country clearances from the Department of State, to track the inventory of passports, to aid travelers in visa applications, to provide reminders to travelers with expired/soon-to-be expired passports to renew and provide separation clearance for individuals offboarding from the EPA (verifying if they have an official passport, and if they do, sending it to the Department of State for disposal).

## Section 1. 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

### 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 hosted in the Agency's Business Automation Platform (BAP), which has a security plan and an Authorization-to-Operate. The current ATO expires July 19, 2024.

### 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.

No information collected or maintained by PENS is covered by the Paperwork Reduction Act (PRA).

### 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 PaaS.

# Section 2. 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, place 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?

Information maintained in PENS is provided by Department of State.

## 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, PENS does not use information from commercial sources or publicly available data.

## 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 Privacy Impact Analysis: 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.

**Privacy Risk:**

There is a risk that information entered into PENS could be mis-keyed.

**Mitigation:**

OITA has a frequent audit process in place to ensure that all information entered into PENS is correct.

**Privacy Risk:**

There is a privacy risk of entering inaccurate data into the system.

**Mitigation:**

The Dept. of State has a review process, as referenced, which serves to mitigate risk OMIS retains the official passports which contains the accurate information and it is cross checked with DOS passport information.

# Section 3. 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 an application built in the Agency's Business Automation Platform (BAP). Access to the controls is maintained via permission set and role-based groups. The Information Management Officer (IMO) and EPA's passport agents, which must be certified by the Department of State have full access to the system. Any request for access would require justification and must be reviewed and approved by OITA's Senior Information Officer (SIO).

### 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 Standard Operating Procedure (SOP) for PENS.

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

Read-only access to limited information (Traveler Name, Passport Location and Expiration Date) for International Travel Coordinators will be created for purpose of Continuity of Operations Planning (COOP) Event response.

If something happens to the travel office, and all the passports at the office are considered lost. The International Travel Coordinators (ITC) in each region and EPA program office would be able to see what passports were at OITA and are now considered Lost and begin working to report and, if needed, replace them.

ITCs are restricted to passport holder's name, the passport location, expiration date and passport holder's region or program office.

### 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, COOP Devolution Designee, approved International Travel Coordinators and the OITA Database administrator will have access to the application on the Agency's BAP. 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 5 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.

Yes. Records in PENS are subject to EPA Records Schedule 1010: Travel Records.

**Privacy Risk:**

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule.

**Mitigation:**

PENS maintains all records with PII in accordance with applicable records retention or disposition schedules approved by NARA or based on the need and relevancy of the data in the support of the OITA mission. Some records are maintained as permanent records due to their continuing historical value; all other temporary records are disposed of in accordance with approved records.

## Section 4. 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.

The information maintain in PENS is not shared externally.

### 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. 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?

Access to system is restricted to few authorized users who uses this information as part of their job duties on daily basis. The PII captured in the system does not have any material privacy impact outside of the person's name and place of birth.

### 5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

All EPA employees are required to complete annual Privacy and Computer Security Awareness Training to ensure their understanding of proper handling and securing of PII. Privacy training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). Leadership at each OITA is responsible for ensuring that all federal employees receive the required annual Computer Security Awareness Training and Privacy Training.

### 5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

**Privacy Risk:**

OITA employees may misuse and inappropriately disseminate information.

**Mitigation:**

An accurate and timely audit process is in place to annually review the physical passport secured in the OITA/OMIS safe and ensure that their information matches what is in PENS.

EPA requires auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed.

EPA employee assigned to maintain the EPA systems have job duties that require them to design, develop, and optimize the system within the security accreditation environment.

Furthermore, each employee is required to undergo annual security awareness training that addresses his or her duties and responsibilities to protect the data.

# Section 6. 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.

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

PENS tracks and manages EPA staffs', who are traveling to foreign countries to conduct official government business, country clearances information. For example, PENS tracks the status of Department of State (DOS) passport applications, official passports, passport numbers, issuance and expiration dates, and the current locations.

## 6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☒ 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.

The passport holder's name will bring up the PENS record which contains the passport number, place of birth, and issue and expiration dates. This system of records is retrieved by name and is covered under SORN: EPA-72.

### 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 goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

OITA has a frequent audit process in place to ensure that all information entered into PENS is safeguarded and secured.

### 6.4 Privacy Impact Analysis: 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 an application on the Agency's BAP containing information copied from physical passports stored and managed by the International Travel Office and Passport Liaisons. There are 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.

**Privacy Risk:**

There is a risk that a user may access information in PENS that he or she does not have a need to know.

**Mitigation:**

To protect the passport information of EPA staff, EPA implemented a series of technical, administrative and physical controls, including encryption to secure transmissions to prevent interception or altercation. OITA is responsible for ensuring only personnel with the

business need-to-know are authorized to access and process information within PENS. In addition, OITA is responsible for ensuring all staff complete EPA's annual security, privacy, record and role-based training and sign the EPA Rules of Behavior (ROB) prior to accessing PENS.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

## Section 7. 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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

### 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 on the passport application form.

## Section 8. 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.

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted.

Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

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

To request a correction of information in PENS, individuals must reach out to OITA letting the office know of the inaccurate information. OITA will take the necessary steps to correct the inaccurate information.

## 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 Freedom of Information Act (FOIA).

**Privacy Risk:**

None. Appropriate procedures are in place to redress the incorrect information.

**Mitigation:**

None.