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: Claims Office Master Files	**System Owner:** Mary O'Lone
Preparer: Mary O'Lone	**Office:** Civil Rights and Finance Law Office, Office of General Counsel
Date: 07/08/2021	**Phone:** 202-564-4992
Reason for Submittal: New PIA____ Revised PIA__X__ Annual Review____ 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 Claims Office Master Files maintain information collected by the Agency to implement the Federal Torts Claims Act, the Waiver Statute (31 USC 5584), the Military Personnel and Civilian Employees' Claims Act, and the Federal Claims Collection Act.

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?

The Federal Tort Claims Act (28 USC 2671 et seq.), the Waiver Statute (31 USC 5584), the Military Personnel and Civilian Employees' Claims Act (31 USC 240 et seq.), and the Federal Claims Collection Act (31 USC 3701 et seq.), including all of their implementing regulations, require information to be submitted to the Agency in order for the Agency to adjudicate individual claims and requests for compensation or debt relief.

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?

[unsure – firewall?]

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.

See Appendix at end of this Assessment.

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?

[unsure]

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).

The data in the hard copy system and in the automated system may include names,

addresses, DOBs, and SSNs. It may also include financial information about an individual's or company's debt owed to EPA or an individual's or company's claim for compensation from the EPA.

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

The sources of information are individuals, including employees, or other entities. It is collected in either hard copy or electronic form.

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.

Data submitters need to provide substantiated evidence in support of their claim, which the office verifies.

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:

The data in the systems may include both sensitive personally identifiable information (SPII) and personally identifiable information (PII) including court orders relating to garnishments, payroll information, leave information, police reports on automobile accidents, financial information, medical and doctor's information related to personal injury claims, the amount of the claim, debt, and/or waiver request, the date of the claim, social security numbers (SSNs), taxpayer identification numbers (TINs), bank account information, driver’s license number, addresses.

Mitigation:

The risks are mitigated through access control levels as described below.

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?

Yes. Only authorized users can access the automated system. The hard copy files are kept in locked file cabinets. The keys are kept by the Assistant General Counsel for Claims, Property, and Appropriations and only authorized staff may use the keys to the file cabinets.

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

They are not documented.

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 authorized users can access the automated system. The hard copy files are kept in locked file cabinets. The keys are kept by the Assistant General Counsel for Claims, Property, and Appropriations and only authorized staff may use the keys to the file cabinets.

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.

The information is retained in accordance with relevant retention schedules. The schedule numbers are 152 and 1025.

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.

Privacy Risk:

The data in the systems may include both sensitive personally identifiable information (SPII) and personally identifiable information (PII) including court orders relating to garnishments, payroll information, leave information, police reports on automobile accidents, financial information, medical and doctor's information related to personal injury claims, the amount of the claim, debt, and/or waiver request, the date of the claim, social security numbers (SSNs), taxpayer identification numbers (TINs), bank account information, driver's license number, addresses.

Mitigation:

The risks are mitigated through the above-described access control levels.

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.

Information may be shared with the U.S. Department of Justice for purposes of securing necessary approvals or in furtherance of defending the U.S. in litigation. Information may also be referred to other federal agencies in the event submissions received by EPA do not belong with EPA.

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

Any external sharing would be in furtherance of carrying out EPA's obligations under the Federal Tort Claims Act (28 USC 2671 et seq.), the Waiver Statute (31 USC 5584), the Military Personnel and Civilian Employees' Claims Act (31 USC 240 et seq.), and the Federal Claims Collection Act (31 USC 3701 et seq.), including all of their implementing regulations.

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?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

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?

Privacy Risk:

The data in the systems may include both sensitive personally identifiable information (SPII) and personally identifiable information (PII) including court orders relating to garnishments, payroll information, leave information, police reports on automobile accidents, financial information, medical and doctor's information related to personal injury claims, the amount of the claim, debt, and/or waiver request, the date of the claim, social security numbers (SSNs), taxpayer identification numbers (TINs), bank account information, driver's license number, addresses.

Mitigation:

Unsure.

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?

Unsure.

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

All individuals with access to the system undergo mandatory records management training that includes how to handle SPII and PII.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

?

Mitigation:

?

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.

The hard copy and automated system are used by the Agency's Claims Officer and OGC attorneys to resolve debts and adjudicate claims under the Federal Torts Claims Act, the Military Personnel and Civilian Employees' Claims Act, the Waiver Statute, and the Federal Claims Collection Statute. If claims information received is misdirected, the Agency will transfer electronically or by mail it to the appropriate federal agency. The automated system provides management information such as summary listings and case status.

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.*)

Data in the hard copy file system can be retrieved by the assigned claim or debt number or by the name of the claimant or debtor. Data in the automated system can also be retrieved by the assigned claim or debt number, by the name of the claimant or debtor, and other limited information that is attributed to the claim, waiver request, or debt. Data cannot be retrieved by SSN or TIN.

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.]
Only authorized users can access the automated system. The hard copy files are kept in locked file cabinets. The keys are kept by the Assistant General Counsel for Claims, Property, and Appropriations and only authorized staff may use the keys to the file cabinets.

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.

Privacy Risk:

?

Mitigation:

?

***If no SORN is required, STOP HERE.**

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.

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?

Providing information is completely voluntary for claim submissions.

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:

?

Mitigation:

?

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 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?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

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:

?

Mitigation:

?

APPENDIX

SF-95 OMB No. 1105-0008 Claim for Damage, Injury, or Death

SF-3881 OMB No. 1510-0056 ACH Vendor/Miscellaneous Payment Enrollment Form

SF-94 OMB No. 3090-0118 Statement of Witness (Accident)

DD Form 2789 OMB No. 0730-0009 Waiver/Remission of Indebtedness Application