



# 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](https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx)

<b>System Name:</b> System Name: eRecovery	
<b>Preparer:</b> Andrew Lam	<b>Office:</b> OCFO/OTS/IMSD
<b>Date:</b> 8/13//2021	<b>Phone:</b> 202-564-2925
<b>Reason for Submittal:</b> New PIA ___ Revised PIA ___ Annual Review <u>X</u> Rescindment ___	
<b>This system is in the following life cycle stage(s):</b>	
Definition <input type="checkbox"/>	Development/Acquisition <input type="checkbox"/>
	Implementation <input checked="" type="checkbox"/>
Operation & Maintenance <input type="checkbox"/>	Rescindment/Decommissioned <input type="checkbox"/>
<b>Note: 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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u></b>	
<b>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</u></b>	

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

eRecovery is used to organize cost information and produce reports that summarize the costs for a specific Superfund Response, Oil Spill site. Additionally, Federal Emergency Management Agency (FEMA) mission assignment costs can be tracked if a specific incident is assigned a site/project identifier or a mission assignment Organization Code. Together the cost report and the supporting cost, and technical documentation will yield a Cost Documentation Package.

## Section 1.0 Authorities and Other Requirements

- 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the system in question?

The federal Superfund law is officially known as the Comprehensive Environmental Response, Compensation, and Liability Act of 1980, 42 U.S.C. 9607; 5 U.S.C. 301; 31 U.S.C. 3512; Executive 9737. The federal Superfund program, administered by the U.S. Environmental Protection Agency, is designed to investigate and cleanup sites contaminated with hazardous substances.

**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?**

The system security plan for eRecovery is being written. An ATO for eRecovery will be obtained prior to being put into production.

**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 ICR Required.

**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?**

No

## **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).**

Include such things as social security number, name, other personal identification numbers, personal information related travel expenses such as home addresses, credit cards, and other recoverable expense items.

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

The primary source of data is from Compass Data Warehouse (CDW) and original source documents. CDW is a repository of Compass data and its predecessor system. The types of information are financial data and associated document pdf images, travel, payroll and voucher data for recovery efforts.

The eRecovery database is a centralized database using Oracle v18.7.0.0. For historical legacy eRecovery data, data is being imported from 11 different schema's (Region 01 thru Region 10 and RTP) to the centralized eRecovery database. The eRecovery database also

has Oracle Database Links (DBLinks) to the CDW that supports a nightly refresh to new transactional data from Compass, PeoplePlus, and Concur travel.

**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.**

eRecovery relies on internal controls in Compass and CDW to ensure accuracy of data.

**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 risk is that the information in eRecovery will be accessed by unauthorized parties.

**Mitigation.**

The eRecovery enforces the most restrictive set of rights, privileges, or access needed by users. eRecovery Security Administrators are required to grant only those rights and/or permissions necessary to perform a given task (least privilege). Access to sensitive data is controlled by the access controls granted to the security group to which each user account is assigned, which then determines where and how a user may navigate within the eRecovery system. Each user has access to the eRecovery data within his/her assigned Region or schema.

## **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, the eRecovery system incorporates group-based access controls that limit the users' rights by what information they need to review or activities they need to perform. The user's role is identified by the employee's supervisor, and approved by regional/national system administrators and then the eRecovery system Security Administrator.

**3.2 What procedures are in place to determine which users may access the**

## **information and how does the system determine who has access?**

The eRecovery system is accessed by only authorized users (EPA personnel, SEE employees and EPA contractors) who work with Superfund cost recovery data that have had a proper background check. Prospective users must complete an appropriate OPM Investigations i.e. (Low Risk Level-NACI; Moderate-MBI; Moderate for IT position-LBI; High-BI) prior to hiring and being granted access to eRecovery. The eRecovery system incorporates group-based access controls that limit the users' rights by what information they need to review or activities they need to perform. The user's role is identified by the employee's supervisor and approved by regional/national system administrators and then the eRecovery system Security Administrator.

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

The eRecovery system incorporates group-based access controls that limit the users' rights by what information they need to review or activities they need to perform. The user's role is identified by the employee's supervisor, and approved by regional/national system administrators and then the eRecovery system Security Administrator. There are no other components other than authorized users.

### **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?**

eRecovery does not allow the public or outside parties to access the system. Only authorized users (EPA personnel, SEE employees and EPA contractors) that have had a proper background check can have access to the system. FAR clauses are incorporated into the applicable EPA contracts. Prospective users must complete an appropriate OPM Investigations i.e. (Low Risk Level-NACI; Moderate-MBI; Moderate for IT position-LBI; High-BI) prior to hiring and being granted access to eRecovery.

### **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.**

In accordance with Records Control Schedule #1036, Superfund cost recovery records are retained for at least 30 years after the completion of all cost recovery at a given Superfund Site.

### **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:**

Potentially the data might be destroyed before 30 years.

#### **Mitigation:**

The current data procedure is not to delete any data at all.

## **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.**

There are 3 categories regarding information sharing for eRecovery: Coast Guard, DOJ, and the Potential Responsible Party (PRP). DOJ and Coast Guard have MOUs. There are 2 Agreement types for PRP: Protective Order Agreement – court order signed by a judge to protect EPA information; Confidentiality Agreement (Agreement between EPA lawyer and other party lawyer).

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

eRecovery Cost Recovery Packages (CRPs), which are shared with the Department of Justice, are a combination of supporting cost and technical documentation. The CRPs are a comprehensive set of documents in which costs associated with a specific site are organized into categories to help EPA recover the costs from potentially responsible parties.

### **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?**

There are 3 categories regarding information sharing for eRecovery: Coast Guard, DOJ, and the Potential Responsible Party (PRP). DOJ and Coast Guard have MOUs. There are 2 Agreement types for PRP: Protective Order Agreement – court order signed by a judge to protect EPA information; Confidentiality Agreement (Agreement between EPA lawyer and other party lawyer).

### **4.4 Does the agreement place limitations on re-dissemination?**

Yes.

### **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:**

Information provided to Coast Guard is raw data (unredacted). The risk is that the information in eRecovery will be accessed by unauthorized parties.

### **Mitigation:**

There are 2 Agreement types for PRP: Protective Order Agreement – court order signed by a judge to protect EPA information; Confidentiality Agreement (Agreement between EPA lawyer and other party lawyer).

## **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 in accordance with stated practices in this PIA?**

The Environmental Protection Agency has the authority to recover costs of response to releases or threatened releases of hazardous substances or discharges or threatened discharges of oil from responsible parties, and also provides necessary supporting documentation for costs EPA has incurred to the U.S. Coast Guard (USCG) to recover costs of response to discharges or threats of discharges of oil from responsible parties. EPA does not have authority to recover costs for oil spill, but the Coast Guard has. This requires preparation of documentation to support the costs incurred and paid, referred to as a Cost Recovery Package (CRP).

There are 3 controls in place to ensure the PII is used in accordance with stated practices in this PIA. First, eRecovery has only data for Superfund and Oil. There is no data for obligations, commitment data etc. Second, eRecovery only grants access to Cost Recovery personnel; those who are involved in the process of Superfund Recovery. And third, EPA reviews the audit logs periodically to identify inappropriate access to PII. An incident response plan is in place for any breaches that involve PII.

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

All users must complete annual Information Security and Privacy Awareness training and role-based training in accordance with NIST requirements.

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

#### **Privacy Risk:**

Compromise data may not be captured if an improper/untimely audit is performed.

#### **Mitigation:**

Annual third-party sufficient assessments are in place to ensure eRecovery data controls are in line with NIST 800-53.

## **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.**

Cost data (and supporting documentation) is integral to cost recovery efforts and required by the federal rules of evidence in litigation. Without detailed cost information (reports & documents) EPA would not be able to recover its cleanup costs from responsible parties. All of this data is essential to the Agency's accurate and timely performance of its cost recovery efforts.

**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.**

Employee identification number (EIN), Name.

**6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?**

EPA- 90

**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:**

Users mishandle eRecovery PII information.

**Mitigation:**

The following procedures are followed to reduce the likelihood of mishandling of PII information: Provide privacy awareness training ensuring that personnel understand privacy responsibilities and procedures. Agency Employees receive annual security awareness training and role-based Privacy training. EPA personnel and contractors are required to complete an Information Security Awareness and Training course on an annual basis. The training course instructs personnel not to disseminate PII information to unauthorized individuals, how to secure information using approved techniques such as encryption, and proper destruction and disposal of PII. Individuals who have system access must have a security background check. eRecovery only grants access to Cost Recovery personnel. Those who are involved in the process of Superfund Recovery.

EPA takes the above steps to reduce the likelihood of mishandling PII information and it reviews the audit logs periodically to identify mishandling of PII. In case PII is mishandled the EPA Privacy Office develops and implements a Privacy Incident Response Plan and provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

**\*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 contain a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA, Attn: Privacy Officer, MC 2831T, 1200 Pennsylvania Avenue, NW, Washington, DC 20460, [privacy@epa.gov](mailto: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?**

Any individual who wants to contest the contents of a record, should make a written request to the EPA, Attn: Privacy Officer, MC 2831T, 1200 Pennsylvania Avenue, NW, Washington, DC 20460.

### **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:**

Notices may not provide enough information for users to understand the full uses of their information.

#### **Mitigation:**

To ensure that the collection notice provide adequate information for users to understand all of the uses for the collection.

## 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 their own personal information in this system of records will be 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 the EPA regulations



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 How does the system notify individuals about the procedures for correcting their information?**

Any individual who wants to know whether this system of records contain a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA FOIA Office, Attn: Privacy Officer, MC2822T, 1200 Pennsylvania Avenue NW., Washington, DC 20460.

## **8.4 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:**

Individuals might be denied requests for PII correction or amendment.

### **Mitigation:**

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.