

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: Response Manager	
Preparer: Brad Morgan	Office: Dallas, TX
Date: 10/13/2020	Phone: 972-977-7422
Reason for Submittal: New PIA_X_ Revised PIA_____ Annual Review_____ Rescindment _____	
This system is in the following life cycle stage(s):	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
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>	
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>	

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

Response Manager is an enterprise data management for EPA On-Scene Coordinators (OSCs) and EPA Contractors. This data management system provides EPA field personnel the ability to manage multiple streams of data associated with the superfund program specifically emergency response and site-specific removal actions. Response Manager is comprised of data modules. Each data module is related to a data stream and the associated data quality objectives for collecting and storing field data.

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?

Response Manager is a data collection application that supports OSCs and other EPA and contractor personnel as part of the Superfund program. The application falls under applicable authorities associated with CERCLA 42 U.S.C. §9601 et seq. (1980), OPA 33 U.S.C. §2701 et seq. (1990), CWA 33 U.S.C. §1251 et seq. (1972), and Stafford Act 42 U.S.C. §5121 et seq.

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?

A security plan has been completed and an ATO has been requested but has not been issued yet.

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?

Yes, data is stored in the cloud using Amazon's cloud service (AWS) in their FedCloud which has gone through the FedRamp certification process. 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).

A summary follows:

- User Account – Includes name, business phone number, business email address which are the PII elements and related to user account info
- Response – Stores data about incident details, photo, evacuations, sources, causes,
- Hazard Eval/Recon – Stores data about orphan containers evaluation and recovery
- Facilities – Stores data including contact information and assessments on impacts to facilities that fall under difference federal regulations like Toxic Release Inventory (TRI), Resource Conservation and Recovery Act (RCRA), Facility Response Plan (FRP), Spill

Presentation Containment and Countermeasures (SPCC), and Risk Management Plan (RMP).

- Spills - Stores data about spills & discharges that are a result of a natural or manmade disaster including oil spills (pipeline, vessels, truck, etc.). It designed to include data on the size and duration of release or discharge and assessment details about the mitigation efforts and remediation of the spill or discharge.
- Drinking Water – Stores data about drinking water systems and current operational status after an incident has affected them
- Waste Water – Stores data about waste water systems and current operational status after an incident has affected them
- HHW – Stores data about Household Hazardous Waste collection pads and number/type of HHW items
- Calls – Stores data about a phone call that relates to the incident
- Shipping – Stores data about shipping containers, shipping manifests, and line items
- Vessels – Stores data about vessels that were impacted by natural disasters and need to be tracked as part of an ESF-10 cleanup. Includes data about the overall status of the vessel including condition and any spills of fuel or oils associated with the Vessel. Also includes identifying information about the vessel and the ultimate disposition of the vessel.
- Properties – Stores data about properties that are in removal/cleaning operations
- Materials – Stores data about materials that may have been contaminated by a constituent
- Contacts – Stores data about contact information
- Data Files – Stores data about documents that pertain to the incident; also allows attaching documents to pieces of data
- Photos – Stores data about photos that pertain to the incident; also allows attaching photos to pieces of data

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

Administrative staff generate login accounts for users. Login is required to view any information in system. Information is collected and recorded to the system in the field via electronic form by EPA OSC staff and their contractors.

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. Neither commercial sources nor publicly available data are used.

2.4 Discuss how accuracy of the data is ensured.

Data accuracy is ensured through adherence to regional and site-specific data management plans. Outlined therein, as required by specific contract. For each individual site there is a

data management plan that describes site-specific quality data objectives and QA\QC processes.

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:

Response Manager collects data in support of Emergency Response and Removal site work. Risk for the collection and storage of data is that the accuracy or mischaracterization of data could lead to negative implications on the usage of the data to support site specific missions.

Mitigation:

Data collected and input into the system is subjected to multiple levels of Quality Control and verification that is driven by the contractually mandated data management plan. These verification processes are updated specifically for each site based on the site Data Quality Objectives and are approved by the OSC or site manager prior to collection of the data.

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?

The system requires secure login as primary access control and implements per module security roles that designate read-only or write access to the content in the given module. There is also an Administrator role with a layer of privileged security access to non-public data and to security management features such as user account creation, role assignment, etc.

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

Access controls are identified within the Response Manager Security Plan, the SOP for User Account Management and the user documentation.

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

There is an administrative role associated with system management duties such as user account management, profile management and application configuration.

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?

OSC employees and designated contractors as determined by OSC. Can also include other state and federal agencies as determined by OSC. Contractor do have the FAR clause in place.

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.

Superfund record schedule is 1036 and has a minimum retention of 30 years. Data that is part of the system becomes part of the administrative record as part of site closeout process and is then moved into the official records management systems.

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:

Information must be protected for as long as it is maintained which depends upon the requirements of a given response event. Longer periods of retention naturally increase the risk of a privacy breach, whether accidental or intentional.

Mitigation:

Create an SOP that establishes a retention schedule for the stored information in RM on the basis of response site requirements and any archival requirements as well. N

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 is not shared unless authorized by regional EPA management and PIO approval processes. Information is shared with third party contractors, as well as state and other federal agencies, in partnership on emergency response efforts where Responses Manager is deployed. Information is accessed through EPA approved PC installations of the Response Manager software.

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

The original business vision for Response Manage expressly lays out the construction of a data management system for use by both OSCs and EPA Contractors to enable the sharing and evaluation of data with EPA partner agencies, state agencies and the public when applicable.

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?

No. Access to info controlled by EPA personnel and request for access must be granted by OSC in charge of the site. Sharing likewise would need to be approved.

4.4 Does the agreement place limitations on re-dissemination?

No

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 Region and EPA Site manager make the determination as to whom to share the information with, done via granting user account access to the system or by exporting/sending reportable data elements in the system. The risk is information may be shared with personnel or entities that do not need to know or have access to the information.

Mitigation:

Access is controlled by login and discrete software installation, which is approved by EPA Site Manager and/or OSC. Site managers and OSCs are EPA personnel and are all required to take annual training regarding privacy and security. Sharing of information is approved by a chain of command starting with the OSC or Site Manager and in some cases going all the way up to the Regional Public Information Officer which verifies that the data is checked prior to approval of sharing to ensure that the recipients are approved and need to know the information.

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 designed around specific data modules and data collection components that enforce the data management scheme intended for the system.

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

EPA personnel are all required to take annual training regarding information security and privacy awareness training which fulfils relevant needs for this system.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Users retain right to access information after period of need has passed (left agency, project ended, etc.)

Mitigation:

The Response Manager SOP for User Account Management establishes the rules for account lifespan, expiration and auditing. A list of all existing RM accounts is generated at the start of each month and distributed to relevant agency leads (EPA and partner agencies). Agency leads are instructed to vet the account list and report back to the Contracting Officer Representative any accounts that should be disabled or extended.

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 system is designed to facilitate the collection and storage of various forms of field data via electronic form or transposed to one. It manages various streams of data in modules for which it provides basic data evaluation, analytical processing, geospatial visualization and delivers custom and automated reports.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No_X_. 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 using a non PII unique identifier for each module of the system. For instance, the system is sometimes used to track properties and this is done by storing the Parcel ID as a unique identifier of the property which is used to retrieve information on the property.

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?

All data is stored on cloud servers that conform to FedRAMP requirement for data security and privacy. Access to the data is provided only through the approved Response Manager client application which must be further approved for installation only by OSCs for site-specific use. The application then also requires an OSC approved user account for authorization utilize data management resources within the Response Manager application. User accounts are terminated as appropriate related to site-specific deployment.

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:

Information collected in association with a response event is subdivided in the system by collection module on the basis of the type of information collected, and users are granted access to specific modules based on the information they need to collect and/or analyze. The EPA Site Manager and OSCs are responsible for making the determination as to which users are granted access to which information modules within Response Manager. Privacy could be breached by providing access to the wrong module(s) or by providing an individual with access who has intent to misuse the information.

Mitigation:

The system has an audit capability that tracks who views, edits, or accesses the information. It also tracks what the previous versions of each record are so any information that is edited, the system tracks who did it and what the previous entry was, so it is always recoverable. Access is controlled by Site Managers and OSCs who have the authority to disseminate information related to their projects. Site managers and OSCs are EPA personnel and are all required to take annual training regarding privacy and security and the potential harm in the misuse of information.

***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.**
- 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?**
- 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?**
- 8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous 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 FOIA.

Privacy Risk:

Mitigation: