United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Response.EPA.GOV	
Preparer: Joe Schaefer	**Office: OLEM/OSRTI/TIFSD/ERT**
Date: 2/27/2020	**Phone: 609-865-8111**
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:

Response.epa.gov is a web-based Content Management System (CMS) used to create mini site profile pages that support emergency response, time critical removals and topics related to the above. Sample content may include site images, documents, Situation Reports (SitReps) (daily activity reports), etc. The CMS is also used to support the National Response Team and some large collection of sites such as the abandoned uranium mines in Region 9.

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?

CERCLA: 42 U.S. Code 9604 Response Authorities (b)(1)

(b) Investigations, monitoring, coordination, etc., by President

(1) Information; studies and investigations

Whenever the President is authorized to act pursuant to subsection (a) of this section, or whenever the President has reason to believe that a release has occurred or is about to occur, or that illness, disease, or complaints thereof may be attributable to exposure to a hazardous substance, pollutant, or contaminant and that a release may have occurred or be occurring, he may undertake such investigations, monitoring, surveys, testing, and other information gathering as he may deem necessary or appropriate to identify the existence and extent of the release or threat thereof, the source and nature of the hazardous substances, pollutants or contaminants involved, and the extent of danger to the public health or welfare or to the environment. In addition, the President may undertake such planning, legal, fiscal, economic, engineering, architectural, and other studies or investigations as he may deem necessary or appropriate to plan and direct response actions, to recover the costs thereof, and to enforce the provisions of this chapter.

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?

Yes, the system has an ATO. The ATO expires on 5/09/2022.

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, the system is hosted at AWS in their FedCloud which has gone through the FedRAMP certification process. It is procured through an IA with DOI to provide EPA IaaS for systems related to emergency response.

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).

Login accounts include Name, Business Phone Number, Business Email address are the PII elements and are related to the user account info and site contacts sections.
There are also fields to identify document and image meta data, and situational reporting information which are typically captured as text fields. There are some other dates like start and stop date for the project

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

Users self-register to create login accounts. By default, only public site profiles and their public information is viewable without a login. Site profile pages are created by OSCs to document cleanup site activities. Profile page web site owners identify which users they want to have access to their site(s) by adding user business email addresses to the Contacts section of their site profile and granting appropriate privileges. Sources of content are the EPA site owners and their contractors. All content is either added or uploaded by privileged users. The EPA Computer Warning Banner about privacy is displayed on the register/login page.

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.

The system does not ensure accuracy of the data as it is supplied by the users and the system cannot verify accuracy of the data.

For new users, temporary passwords are sent to the registered email address. For existing users, a forgotten password request only allows a password reset. A link to reset passwords are sent to the registered email address. If user accounts are locked out or expired due to inactivity, user must contact Administrators for assistance.

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 low risk of inaccurate information due to human error.

Mitigation:
User's verify their information prior to account creation.

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. There are three levels of access, Public, Private and Exclusive. These are the different levels of security on the site content. Based on the level defined by the user, the content's visibility is limited to logins that have those privileges.

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 web site owner/OSC determines who (i.e contractors, local, state, etc.) and what level of access users may have on their site profile pages. The content on the pages are configured with different levels of security. Based on the security level of the ser (as defined by the site owner/OSC), the content's visibility is limited to logins that have those privileges. Users of their site profile pages are managed in the Contact Manager section of that site and is specific to that site. Access levels are documented in the EPAOSC User Guide.

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

A site owner has access to modify the site content and adjust rights including granting other personnel access to that particular site.

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?

Site stakeholders as designated by the EPA On-Scene coordinator or Remedial Project manager who act as the site owner, may designate individuals to access all or part of the site. All support contractors who are designated have the appropriate FAR clauses to the best of my knowledge.

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.

This site supports the Superfund program and ultimately falls under EPA Records Schedule 1036. Records are retained for possible lawsuits against a company for illegal environmental activities and will be retained for at least 2 years after the data is no longer needed.

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 may be retained longer than it is needed.

Mitigation:

While we are working to directly integrate with the Superfund Enterprise Management System (SEMS) site owners are ultimately responsible for ensuring that all content they had added to their site is also delivered to the superfund records system as part of their administrative record.

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.

Response.EPA.GOV does not have any standing data connections with non-EPA entities. On a site by site basis, the Federal On-Scene Coordinator or Remedial Project Manager may allow access to non-EPA personnel. This is following the Regional practices they use to work with site stakeholders and enable access to information on the site.

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

EPA SORN 74 states that "Records may also be disclosed to public health authorities in conformity with federal, state, and local laws when necessary to protect the public health or safety, or to federal, state, or local governmental agencies when it is determined that a response by that agency is more appropriate than a response by the EPA" The method that response.epa.gov implements of allowing the EPA project lead to make that determination is consistent with what's identified in the SORN.

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?

That is done at the regional level on a site by site basis.

4.4 Does the agreement place limitations on re-dissemination?

The superfund site team would work out those details on a site by site basis and then utilize the system to match that agreed upon approach.

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:

There is a minimal risk of potential exposure to PII. The information could potentially be shared with someone who did not need access to the information.

Mitigation:

Access to the system is role based. There is a user agreement in place instructing users to adhere to the rules of behavior.

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 (Section 6.1)?

The system has an audit function. Response.EPA.GOV is configured to audit Account Login events for successes and failures to ensure that the user accounts are being used as intended.

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

EPA users and contractors receive the standard agency yearly security and privacy awareness training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk data not being accounted for due to improper audit.

Mitigation:
There are audit logs in place

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 uses the information to identify who is working on a particular project and control access to information contained on the site.

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.)

The primary way information is retrieved is by selecting the site name from the site list and then that presents the profile page for the site with links and previews of the other section. Users can only access the sites on which they have privileges and only have access to their own user account information.

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

If the site deals with a residential cleanup, EPA SORN 74 – Environmental Assessment of Residential Properties would come into play and cover the content that is posted on the site which would typically be reports uploaded as documents

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:

The risk is potential unauthorized use of information.

Mitigation:

PII is verified through the account creation to ensure that PII is only used for the purpose of collection.

*If no SORN is required, STOP HERE.

Enter any content that you want to repeat, including other content controls. You can also insert this control around table rows in order to repeat parts of a table.

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

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:

Mitigation: