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:** Superfund Enterprise Management System (SEMS) | **System Owner:** Steven Wyman |
| **Preparer:** William Bushee | **Office:** OLEM/OSRTI/RMD/IMB |
| **Date:** May 16, 2023 | **Phone:** 202.566.1126 |
| **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 ☐<br><br>**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).**<br><br>**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 SEMS database application supports the electronic capture, imaging, indexing, and tracking of records which document investigation, cleanup, and enforcement activities at potential and existing hazardous waste sites, as mandated by the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA) of 1980, as amended by the Superfund Amendments and Reauthorization Act (SARA) of 1986, known collectively as CERCLA.

SEMS is a key EPA asset used to meet responsibilities of Federal agencies, Congress, and the Public in Superfund site remediation and cleanup, and emergency response support. It addresses the Agency's

performance gap for capturing, preserving, and disseminating legislatively mandated Superfund documents and records. SEMS is an electronic repository of Superfund documents routinely used to disseminate records in response to Freedom of Information Act (FOIA) requests, Administrative Records (ARs), and for litigation support. SEMS advances e-Government by providing reliable and easily accessible documents to citizens for use in making more informed decisions in their communities. Beneficiaries of content exported from SEMS include citizens, States, Tribes, Congress, and the business community.

A fundamental objective of SEMS was to evolve the primary Superfund data collection, reporting and tracking modules— Site Management (SM) and Records Management (RM) into one single integrated system, leveraging the capabilities and strengths of the predecessor systems while eliminating the redundant design features, data collection efforts and maintenance activities. The result is a one stop source for Superfund data collection and tracking activities. The decision to move forward in the integration of existing core Superfund Management systems into a single SEMS was chosen to close the performance gap for capturing, preserving and disseminating legislatively mandated Superfund documents and records.

As SEMS progresses through its lifecycle, additional modules will be added that enable geo-locational representation, permit retrieval of analytical data, and offer new customer user interfaces. SEMS will reduce redundancies by consolidating Superfund site level searches, sharing information sources, and simplifying site searches – all within a single system. SEMS will also take advantage of enterprise architecture components such as the EPA Enterprise Architecture (EA) and service-oriented architectures as it matures.

SEMS will provide better service to citizens by establishing strong information management controls, cross-platform search functionalities, and efficient content delivery. SEMS will form a flexible and adaptive technological framework in support of program decision making and lines of business.

# 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, as amended by SARA – The Comprehensive Environmental Response, Compensation, and Liability Act (Public Law 96-510), and the Superfund Amendments and Reauthorization Act (SARA- Public Law 99-499)
- CWA, as amended by OPA – 1972 Clean Water Act, amended by Office of Public Affairs (OPA), NCP 40 CFR Part 300.
- Executive Order 12777 – Delegate Presidents authority for responding to discharges of oil and hazardous substances under the CWA and OPA to the EPA and US Coast Guard
- Executive Order 12580 and 13016 - Further delegated authority to releases of hazardous substances under CERCLA to the EPA, USCG, DoD, DOE, and other federal agencies.
- OMB Memorandum 99-18, *Privacy Policies on Federal Websites*, June 1999.
- OMB Memorandum M-03-22: *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
- OMB Memorandum 99-05: Attachment A: *Privacy and Personal Information in Federal Records* and Attachment B: *Instructions for Complying with the Presidents Memorandum of May 14, 1998*, "Privacy and Personal Information in Federal Records."

- Government Paperwork Elimination Act (GPEA), Public Law 105-277, Title XVII, October 21, 1998.
- The Paperwork Reduction Act of 1995, Public Law 104-13, May 1995.
- The Privacy Act of 1974, Public Law: 93-579, September 1975.

### 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 ATO expires August 2023

### 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 - we collect data internally concerning sites, and not from the public

### 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. Currently the application is not in a cloud environment, it is hosted at the NCC. However, we are in the process of migrating to the NCC AWS cloud, utilizing IaaS.

## 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).

SEMS will contain data/information that supports program activities and decisions regarding cleaning up specific Superfund sites and is intended to provide repositories of or access point to a variety of program data including site management, cost recovery, site financial information, enforcement actions, and supporting documentation.

Data elements collected are as follows: Site location, basic descriptive information; contact information (e.g., name, address, telephone number, email address) for key individuals with responsibilities on specific Superfund sites; data generated by EPA in regards to site information and actions conducted at the site; planned and actual site financial and enforcement information; potentially responsible parties (PRP); negotiation data; litigation/referral data; lien data; alternative dispute resolution data; litigation history; correspondence tracking; community involvement data (i.e., location, contact data, technical assistance grant data); and medical information pertaining to environmental sampling results or public complaints.

As the SEMS solution will be integration of existing Superfund systems and their respective information, the information may include correspondence, reports, laboratory

analyses, FOIA requests and responses, photographs, technical drawings, maps, and digital audio/video clips that are specific to the Superfund, Brownfields, Emergency Response and Prevention, Cost Recovery, Enforcement and other delegated/non-delegated EPA programs with ties to the Superfund program.

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

Information that will be captured in SEMS is derived from a variety of sources, including existing programmatic records, Agency staff and contractors, civil investigators, attorneys, and the like.

Those with responsibilities for site cleanup and management submit data and records to the system. Those with such responsibilities include site assessors, remedial project managers, on scene coordinators, enforcement officers, attorneys, financial analysts, and others. The data come from a wide variety of sources

## 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.

SEMS ensures data is accurate through the following:

- Annual data control entry plans are submitted to provide a consistent plan for entering and maintaining current, complete, consistent and accurate data in Superfund systems and relevant and timely data to the public.
- Cross checking data entered through reports
- Deploy business intelligence tools to review data
- Assign data sponsors that understand and review segments of the data regularly through analysis and reporting

## 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 privacy risks related to the characterization of the information include risks regarding enforcement sensitive information and planning information. Low risk of providing access to information to people without the need to know

**Mitigation:**

- Access to the system is extremely limited to EPA staff and contractors working on Superfund related work. No one is provided access to the application without a need-to-know and approval of supervisor via user form.

- Accounts are assigned from EPA Headquarters who have personal knowledge of each individual's need to access the information in the system.
- There is a privacy/warning notice that is displayed on each login.
- Each user must log in with a username and password each time they access the system

## 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, users are assigned roles and privileges by the system administrator in the regions who manage and control access to the various applications, modules, and forms in SEMS. The System Administrator role will determine which users have access to the SEMS applications, and within an application, which forms, functions, and reports a user can access. Before a user is granted access, they must complete a new user form and signed by their supervisor. Staff are then assigned particular roles, and through these roles assignments, they acquire rights "permissions" to perform particular functions.

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

Before a user is granted access, they must complete a new user form and signed by their supervisor. Staff are then assigned particular roles, and through these roles assignments, they acquire rights "permissions" to perform particular functions. These procedures are documented in the security plan under Appendix F: Account Management.

### 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?

The current SEMS contract, NITACC, include the FAR and Privacy clauses

### 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.

Because SEMS information is used for cost recovery purposes, information is retained for a 30-year period after the cost recovery timeframe has ended. The RCS is 0052, 0061, and 1036.

### 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:**

- Residual privacy risks are mitigated by limited access to the data, non-portability of the data and controlled storage of the data in controlled facilities.
- Retention of application-specific data is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the record schedules.
- Employ least privilege principles to data access
- Review Audit logs to ensure data is not intentionally deleted or altered

**Mitigation:**

We do not give access to this data to anyone outside the Agency. Access controls are in place to restrict access to the data to specific internal Agency personnel only. If an individual who has permission to access this data chooses to export the data and share it on their own, they are violating not just SEMS guidelines but also US Federal Statutes including Privacy Act, Records Act, and various US Code statutes.

# 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 routinely shared outside the Agency to the public through two mechanisms:

- Public submits a FOIA request through the FOIA office and tracked through FOIAonline or
- Disseminating information via EPA public websites. The basic steps to publish content to the EPA website are:
  - ✓ Subject Matter Experts (SMEs) adding/updating content

- ✓ Reviewer assesses, and approves or rejects updates
- ✓ Publishers advertises content to the public web

Information shared with DOJ for litigation purposes, have a special process and are championed by an attorney. The current process is as follows:

- ✓ Request comes in from DOJ to the EPA.
- ✓ An Email is generated identifying the program office and all internal POCs associated with the request
- ✓ Identify potential data sources and criteria - Criteria includes people, topics and themes associated with the complaint
- ✓ Perform EnCase search and review results and next steps
- ✓ Gather results and encrypt information on CD
- ✓ Attorney distributes information to DOJ

Process is governed by the EPA information collection policy - Collection and Retention Procedures for Electronically Stored Information (ESI) Collected Using E-Discovery Tools (EPA Classification No.: CIO 2155-P-3.0)

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

The information shared/disseminated is to provide the public with information regarding Superfund sites in their areas and can be used for research and/or general purposes.

## 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?

Information sharing agreements are reviewed annually during their annual risk assessments. Also, since SEMS is an internal application with no public access. Information is reviewed prior to releasing data to the web for public consumption.

## 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:**

Given the **internal sharing**, discuss what privacy risks were identified and how they were mitigated.

The fundamental privacy risk lies in unauthorized disclosure based on methods of sharing. 8

The two methods and the mitigation of potential risks are as follows:

- Information delivered by courier or hand-carried is subject to media labeling controls. Transport of this information is subject to EPA controls for media transport.
- E-mail is subject to the Agency's infrastructure security controls., and
- Where appropriate, Memorandum of Understanding/Interconnection Security Agreement is in place

The predominant privacy risk attributable to **external sharing** data with the public lies in a breach to confidentiality.

**Mitigation:**

The two methods and the mitigation of potential risks of **internal sharing** are as follows:

- Information delivered by courier or hand-carried is subject to media labeling controls. Transport of this information is subject to EPA controls for media transport.

In order to ensure that the information is used as stated in section 6.1, audit tables are in place which track changes/deletions to the database.

- SEMS uses the Agency ArcSight and Symantec EndPoint Protection. SEMS will be moving to the new Continuous Diagnostics Tools as they are implemented across EPA for more in-depth monitoring and auditing E-mail is subject to the Agency's infrastructure security controls., and
- Where appropriate, Memorandum of Understanding/Interconnection Security Agreement is in place

To mitigate the **external sharing** risk, OSRTI has instituted several technical, operational and management controls. Secure transfer protocols are deployed in the transmission of information to the web.

# 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?

In order to ensure that the information is used as stated in section 6.1, audit tables are in place which track changes/deletions to the database.

SEMS uses the Agency ArcSight and Symantec EndPoint Protection. SEMS will be moving to the new Continuous Diagnostics Tools as they are implemented across EPA for more in-depth monitoring and auditing

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

All authorized users of the SEMS application are required to take the Agency's Annual Information Security and Privacy Awareness Training. an annual security training

identifying the user's role and responsibilities for protecting the Agency's information resources, as well as, consequences for not adhering to the policy

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

- Authenticator/Password Management -- Application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators.
- Account Management -- Application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review, all of which support implementation of need-to-know.
- Access Enforcement -- Application and monitoring of access privileges.
- Least Privilege -- Provision of the minimum tools required for a user to perform his/her function.
- Unsuccessful Login Attempts – SEMS automatically locks the account until released by a System Administrator when the maximum number of unsuccessful attempts is exceeded.
- Audit trails are generated by the SEMS application. The audit trails facilitate intrusion detection and are a detective control for identifying data misuse. SEMS is also configured to protect audit information and tools from unauthorized access, modification and deletion. Audit notifications are generated in response to pre-specified triggers

**Privacy Risk:**

The risk is low due to the auditable events and audit logs being reviewed and analyzed by Agency personnel and system owner.

**Mitigation:**

- The Agency enforces the reliability and integrity of operational information, and is in compliance with all applicable Federal laws, regulations, and procedures to ensure the safeguarding of Agency assets.
- The NCC provides scans within Agency defined time frame: Requested Scans and are delivered and reviewed:
  - ✓ Tenable Scan - Provided Monthly, with weekly updates from ISO
  - ✓ WebApp Scan - Every 72 hours
  - ✓ Credential Scans - Every 72 hours
  - ✓ Splunk Scans- Every 72 hours

## 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.

SEMS information will be used in a variety of ways: research, enforcement and compliance, litigation support, responses to Congressional and FOIA requests, public participation in the Superfund process, electronic archiving, cost recovery, disaster recovery, and support of the program/Agency mission

**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.*)

SEMS information is retrieved by the site id number or site name.

**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.*]

SEMS collects non-sensitive information on individuals in one of two ways. First, it collects information on Site Contacts (EPA points of contact). Information entered into the database is Name, Affiliation Type (Toxicologist, PRM, Attorney, etc), Region, Email Address, and Primary Contact. This information is publicly available on the Superfund Home page, under Superfund Sites Where You live, then under Site Contacts.

The second instance is Primary Responsible Party (PRP). Collected information contains Party Name, Site Name, EPA Id, Site Address, NPL Status, Non-NPL Status, Involvement and Liability Type. This data is not publicly available until the Parties have been issued a general or special notice letter and/or are a party to an enforcement instrument. The site name, site address, party name, EPA ID, NPL Status, Non-NPL Status are made available to the public through the FOIA 11 report.

PII may be contained in some documents stored in the document repository. Such data can be retrieved only by full text search criteria. Personal identifiers can be retrievable in SEMS unless they have been permanently redacted from the electronic file, though no specific search fields for PII exist. The system is designed to capture information about sites, not individuals, therefore users will primarily retrieve information by Site Name or EPA Site Identification Number.

## 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.*

FYI: SEMS currently has a SORN (EPA-69)

**Privacy Risk:**

The information might be misused, not redacted, or disseminated to unauthorized users

**Mitigation:**

There are limited access rights depending on user role. The PO during his/her review will ensure that the information is being properly used. All users, prior to providing access, must complete a new user form, signed by their supervisor. The user form identifies the roles/privileges the user will assigned.

SEMS monitors the Privacy information to comply with privacy protection requirement. Audit tables are in place which track changes/deletions to the database.

The SEMS users as any other EPA personnel or contractors are required to complete the Agency's General Privacy Awareness Training course on an annual basis. They are required to comply with EPA establishes privacy roles, responsibilities, and access requirements. SEMS Program Manager and System owner establish system-specific privacy roles, responsibilities, and access requirements for contractors and service providers; and requirements for contractors.

SEMS users are instructed not to release agency data classified as PII/Privacy Act (PA)/Controlled Unclassified Information (CUI) to unauthorized users.

SEMS uses the Agency ArcSight and Symantec EndPoint Protection. SEMS will be moving to the new Continuous Diagnostics Tools as they are implemented across EPA for more in-depth monitoring and auditing.

***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?

Request for access must be made in accordance with the procedures described in EPA's Privacy Act regulations at 40 CFR part 16. Requesters will be required to provide adequate identification such as driver's license, employee identification card, or other identifying document. Additional identification procedures may be required in some instances

### 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:**

Low (minimal) risk of inadequate notice.

**Mitigation:**

The notice is in place on the portal page containing the data and the consent functionality was put into place in December 2017 as part of the FR 12.3 release.

# 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:**

Low (minimal) of users not being aware of how to correct inaccuracy of their data.

**Mitigation:**

There is appropriate process in place to correct inaccurately. If there is something inaccurate/incorrect Supervisors, Regional Information Management Coordinator's (IMCs), Subject Matter Experts (SMEs), and Training to verify and correct user Data or will ask user to correct their data.