# 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:** Emergency Management Portal (EMP) | **System Owner:** Rob Thomas |
| **Preparer:** Rob Thomas | **Office:** Office of Emergency Management |
| **Date:** 06/26/2024 | **Phone:** 202-564-7507 |
| **Reason for Submittal: New PIARevised PIAAnnual Review_X 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:

EMP is an internal webpage-based gateway & security solution that houses a suite of 2 application modules and 4 software tools: Field Readiness (FR or FRM), Oil Database (OdB), EMBI (Emergency Management Business Intelligence) Reporting tool, Incident Management Handbook, EMPAdmin, and Document Library. The two-flagship database management application modules: Field Readiness and Oil Database are used during Emergency Response as well as in every day Regional & Headquarters'

activities pertaining to Inspections, Removals, Monitoring, Laboratory examination, Compliance, Enforcement, etc. Both FR and OdB are capital management application modules used for Decision Support programs used for the management and tracking of Agency and non-Agency capital resources such as readiness of human beings (FR) and proper operation of Petro-Chemical/Chemical facilities.

## 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?

- Executive Order 13650 on Improving Chemical Facility Safety and Security,
- Emergency Planning and Community Right-to-Know Act (EPCRA),
- Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA),
- Water Act of 1984,
- National Contingency Plan Subpart J (Product Schedule, Emergency Response & Clean-up Actions),
- Big Data Act,
- Management of Government Technology, Program Management Integrity Assurance Act (PMIAA).

### 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. Yes. July 2023; received another extension until October 31, 2024.

### 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; there are no multiple forms.

### 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, not applicable. EMP is maintained at NCC-East, RTP North Carolina.

# 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).

EMP system, particularly the FR & OdB application modules collect CBI/CUI (Confidential Business Intelligence/Controlled Unclassified Information) in the form of High Value Asset (HVA), Sensitive-Personal Identifiable Information (S-PII), and Personal Identifiable Information (PII) data.

That information in FRM can consists of work & home address; work & personal email; work, home, & cell phone numbers; work, personal, medical, & emergency contact information including emergency contact name/relationship; fit-test, immunization, medical examination related information, and DOB for members of On-Scene Coordinators (OSCs), CID (Agents, Inspectors, Compliance Officers), Scuba Divers, Laboratory personnel, Environmental Team, Removal Management, Water and Aircraft operators, Safety & Health, Remedial Program Management, Response & CBRN Teams, and Response Support Corp (RSC) of EPA HQ's and Regional federated operational resources.

That information in ODB consists of operator company name, operator contact name, operator address, geographical location, mailing address, owner company name, owner company contact name, owner company address, owner phone number, owner address, facility address for petro (Oil) & chemical facilities, facility type (SPCC & FRP Facilities), chemical substance, storage type, storage size, spill data, hazardous material, high risk designations, closest body of water, fossil fuel wells, compliance status, court date(s).

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

Manual entry of all data will be done by Agency employees mostly Data Managers (Including SHEM), RSC Coordinators, Training Coordinators, CID Leads, Inspector Leads, Oil Program personnel, or

Environmental Responders themselves (i.e., OSCs, Inspectors, Divers, etc.). Note: User profiles such as (Data) Managers or Coordinators have power-user permissions/rights which gives them access to a respective employee's records for that perspective Region(s) or AA-ship(s) in order to make updates etc... pertaining to programmatic operations.

### 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, EMP does not.

### 2.4 Discuss how accuracy of the data is ensured.

Each Agency Region, AA-ship(s), or Program Office has Data Managers (Removal, RPM, CID, and/or SHEM) or Coordinators (RSC or Training) that verifies the accuracy of the data inputted into EMP-FRM.

### 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 risk of inaccurate information and compromise of PII and SPII.

**Mitigation:**

On protection of PII and SPII, we deploy privacy controls from NIST SP 800-53 control catalogue. As for accuracy, the data is voluntarily input by users directly or by a data manager or supervisor on the employee's behalf. If any data is inaccurate, users or data managers update the data to the correct information.

## Section 3.0 Access and Data Retention by the System

### 3.1 *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.* 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, it has access control levels. User rights, permissions, and group designations are in place. Access control to user records is governed by

security group membership, which is managed by the OEM's EMP System Owner and EMP Help Desk in conjunction with the process and procedures of the Agency's Enterprise Web Access Management System. Only supervisors, data managers, data entry, and RSC Coordinators have access to the personal, medical, emergency contact, and facility information.

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

User rights, permissions, and group designations are in place for proper data access. The system determines who has access by group designations with permissions and rights assigned to each user by the contract developers directed by the COR and/or system manager of the web system.

The procedure is standard NCC Hosting policy and/or infrastructure for program office computer systems such as EMP to make system request calls to Agency Enterprise Authentication System in order to receive organizational and access/authentication data pertaining to user(s) security roles.

## 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?

EPA employees (HQ's & regional) and contract developers. EPA employees, such as users, supervisors, data Mmanagers, & coordinators have access to their own record. In addition, Supervisors, Data managers, & coordinators have access to records of field operations employees within the system. When the user specifies their supervisor, that supervisor has access to the information. Contract Developers develop, enhance, maintain, and troubleshoot the application code. The NCC Hosting contractors deploy and back up the application system and its data.

Yes, FAR Privacy Act clauses are included in the ITS-EPA IV contract.

### 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.

Information is retained only as long as the person is a member of either profile(s): Job title,

expertise & skills, special teams or groups, a member of physical field activity operations, or until the person has left the EPA.

Yes. EPA RS-0757

### 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:**

There is a risk of retaining data beyond the authorized period.

**Mitigation:**

EMP system and Agency personnel perform bi-weekly to monthly reviews of personnel roster. When there is a discrepancy with the data, EMP and/or Agency personnel alert the system's helpdesk. After which the system personnel carry out actions to correct the discrepancy i.e., deactivating an employee who no longer is with the agency.

## 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.

No. (Only selected data is shared with OMS data share programs i.e. FTP-Secure (GoAnywhere server) for internal Agency usage i.e. EDG, FRS, Qlik Sense, etc).

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

N/A

### 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?

The System Manager, Information System Security Officer (ISSO), Information System Privacy Officer (ISPO), Project Officer, & COR consults with other Agency professionals of like stature to discuss the sharing of data for mission critical reasons, what data is (actually) needed, and how the data is to be transferred in accordance with statutes, policies, and an active SORN FRL-9926-37-OEI; EPA-HQ-OEI-2014-0758; EPA-70.

### 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:**

Not applicable.

**Mitigation:**

Not applicable.

## 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 has an audit system in place to track user's creation and modification of data. EMP personnel review the audit logs on periodic basis i.e., monthly, quarterly, annually. Risk Management Framework is used to manage risk and security information. We conduct assessments to assess risk periodically, maintain required logging practices and continuously monitor information use and system configuration.

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

OLEM does not provide privacy training specifically for EMP's users concerning data collection before gaining access to the system. OLEM relies on the Information Security and Privacy Awareness Training that's taken annually by all EPA employees.

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

**Privacy Risk:**

There is some risk likely to arise due to untimely audit of user usage.

**Mitigation:**

Audit logs are used to enhance supervision checks and audit trails to report all access and operation of the system. Periodic risk assessments are done. Continuous monitoring performed and OIG oversight conducted. EMP personnel have developed a popup window to appear on the computer screen for data managers after they have logged into an EMP application module to improve or adhere to timely audits of user usage.

## 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 EMP system's application modules along with its associated reporting tool enable approved users to review data on employees (human capital) to determine their level of readiness with respect to the requirements of (particular) every-day field operations, emergency response deployments, inspections, or exercises. This implementation of technology helps to determine the level of readiness for Agency human capital resources to respond to environmental incidents, to plan for future readiness or preparedness needs, to carry out everyday field operation activities, and for programmatic performance measurement needs.

EMP system's Field Readiness serves as a web-based, centralized, nationally consistent platform for recording training completion, certifications, fitness tests, deployments, exercises, and medical examinations as well as immunizations & fit tests that are associated with everyday field operations, inspections, emergency response deployments, and health & safety statuses.

The personnel and emergency contact information are being collected so the personnel's supervisors can contact them in case of an environmental emergency or other field operation event that may require their involvement. Also, if personnel are activated or tasked i.e., RSC, N-IMAT, ERT, etc. the person's emergency contact information may be used in case of an emergency activity involving the individual.

The restricted medical information i.e., fitness test, respiratory, immunization, physicals, etc. are collected to determine if the human capital is fit or medically cleared to deploy or work in the field for emergency environmental incidents and/or programmatic operations.

## 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.*)

Information is designed to be retrieved by username, EPA email address, EPA organization, or EPA LAN Account. This is to view: certifications, trainings, exercises, response deployments, and restricted medical information.

## 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?

Privacy risk is assessed during the PTA process, periodic PIA process as well as the Continuous Monitoring Assessment process by third party. The SORN process provides an additional opportunity to evaluate risk to individuals.

## 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:**

There is some risk of data misuse in the application modules.

**Mitigation:**

EMP has procedures in place to regulate granting of user permissions and depending on permissions granted, the application allows or restricts access to the information. User rights, permissions, and group associations are in place. Access controls to user records are governed by user rights, permissions, and security

group membership, which is managed by the OEM's System Manager and EMP Help Desk after authentication and account validation via the Agency's Enterprise Web Access Management (EWAM) system. Besides users' ability to see their own data; supervisors and data managers (i.e., Removal, RPM, & SHEM), and coordinators (i.e., RSC & Training) have access to thepPersonal, medical, and emergency contact 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.

Users access and view Privacy Act Statement at log on. Prior to this, the SORN process provides an additional opportunity to users to raise objections, if any.

### 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 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 2810A, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

Request for access must be made in accordance with the procedures described in EPA's Privacy Act regulations at 40 CFR part 16 and EPA's modernized Privacy Act Request Procedure. 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:**

There is some risk that notice is inadequate.

**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 can access their information to obtain a copy, request an amendment or consent to share through the Privacy Act Request Procedure. 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.

Access to the personal and emergency contact information is limited to the person himself/herself; the person's supervisor, as listed in EMP-FR; and the person's organizational Data Managers, RSC Coordinators and their specific designees.

## 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:**

There is some risk that users lack awareness of how to correct inaccuracy of their data.

**Mitigation:**

There is appropriate process in place to correct inaccurately entered data. If there is something inaccurate/incorrect supervisors, regional data managers (Removal & SHEM), and coordinators (i.e., RSC, Training) verify and will correct user data or will ask user to correct their data.