![EPA 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: **Emergency Management Portal (EMP)**	
Preparer: Rob Thomas	**Office: Office of Emergency Management**
Date: 07/19/2019	**Phone: 202-564-7507**

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:

EMP is an internal webpage-based gateway & security solution that houses a suite of 3 application modules and 3 software tools: Field Readiness; Oil Database; Local Governments Reimbursement; EMBI (Emergency Management Business Intelligence) Reporting tool; Incident Management Handbook; and EMPAdmin. The two flagship applications: Field Readiness (FR) and Oil Database (OdB) are used during Emergency Response as well as in every day Regional & HQ activities pertaining to Inspections, Removals, Monitoring, Labs, etc. FR and OdB are Decision Support Systems (DSS) used for the management of Agency and non-Agency capital resources.

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?

Privacy Act of 1974 (Public Law 93-579), Executive Order 13650, EPCRA, CERCLA, Water Act of 1984, National Contingency Plan Subpart J Product Schedule, Emergency Response & Clean-up Actions

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 2020.

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?

Maintained at NCC.

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, particularly the Field Readiness application module, collects personal & emergency contact information for EPA HQ's and Field personnel. Such as On-Scene Coordinators (OSCs), Inspectors, Scuba Divers, Laboratory personnel, Environmental Team members, Removal group members, water and Air craft operators, and Response Support Corp (RSC) group members. That information can consist of: home address, personal email, home and cell phone numbers as well as emergency contact name, relationship, and phone numbers, home address, and email etc.

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 the Agency employees mostly Data Managers (Including SHEM), RSC Coordinators, Training Coordinators, 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.

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 doesn't.

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

Each Agency Region and AA-ship(s) or Program Office has a Data Manager (Removal and/or SHEM) or Coordinator (RSC or Training) that verifies the accuracy of the data inputted into EMP-FR module.

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:

Low (minimal) to none. 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 can simply update the data to the correct information.

Mitigation:

1) Restriction of access to the privacy related information is restricted only to the user themselves and/or specific Data Managers within the Program Office or Region. 2) The list of data managers with this data access is small and restricted to a list that is pre-approved by SHEM, OEM (i.e. Response Support Corps (RSC)), OECA, and Regional program officials in the Agency.

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, 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 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, and RSC Coordinators have access to the Personal and Emergency Contact information.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

User rights, permissions, and group designations are in place for proper data access. The system determines who has access by permissions, rights, & group designation 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 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 Managers, & 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. NCC Hosting contractors deploy and back up the application system and its data.

Yes, FAR Privacy Act clauses are included in the ITS-EPA III 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 profiles: Job title, Expertise & Skills, Special Teams or Groups, a member of physical field activity operations, or until the person has left 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:

Low (minimal) to none. Regardless of the length of time data exists in the system, the system access controls are still in place to restrict access to the data at both the user and NCC data center level.

Mitigation:

Information is archived to a non-accessible database table when an employee who resigns as a member of any group, team, or has field operations responsibilities i.e. Response Support Corps. Additionally, a process and action items were put in place in December 2017 to archive the data of anyone who has left the Agency without resigning from the EMP- FR module.

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 exported out via ODBC to an internal Agency Data Analytics application, Qlik Sense.

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, ISSO, System Privacy Officer, 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 to statutes, policies, and active SORNs 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:
Low (minimal) to none.

Mitigation:
We do not give access to this data to anyone outside the Agency. 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 EMP guidelines but also US Federal Statutes including Privacy Act and various Records Act.

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 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.

EMP was developed to use the information in accordance to the practices on the PIA, PTA, and National Privacy Program (NPP) On-site Review. Contract developers and EPA Agency employees are contractually constrained by the Security Policies &/or statutes, FAR, and Privacy Act statutes &/or clauses in their employment contracts.

To be transparent the EMP system and it's application module, Field Readiness (FR) is not able to make sure Agency employee use the data as stated in 6.1 if the data is exported out of EMP-FR directly (database connector) or indirectly (manual export). Unless the system data stays inside EMP-FR, then system can contain and ensure the data is used as stated in 6.1.

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

OEM does not provide privacy training specifically for EMP system's Field Readiness application module users concerning the system/collection before gaining access to the system. OEM relies on the Agency required Privacy training that's taking by all EPA employees.   Yet a link to the Privacy policy is located near the top of the personal and emergency contact information input page in the Field Readiness Application module.

5.3   Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:
Low (minimal) to none. If users do not take the annual Agency privacy training and do not use the data properly.

Mitigation:
All users authorized to use the system are expected to complete annual Agency required Privacy training. In additional contract software developers are expected to complete the Agency required Privacy training annually. The Agency will shut off network access for anyone that does not complete the

training.

EMP was developed in accordance with its specific requirements and nothing beyond the stated user requirements are in place. Errors would flag and inhibit functionality if a user was trying to misuse the system.

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.
EMP-Field Readiness serves as a web-based, centralized, nationally-consistent platform for recording training completion, certifications, fitness tests, deployments, exercises, and medical examinations associated with every day field operations, emergency response deployments, and health & safety statuses.

The EMP System and its 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 and emergency response deployments or exercises. This implementation of technology helps to determine the level of readiness for the Agency human capital resources to respond to environmental incidents, to plan for future readiness or preparedness needs, to carry out every day field operation activities, and for programmatic performance measurement needs.

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 user name, EPA email address, EPA organization, or EPA LAN Account. This is to view: certifications, trainings, exercises, and response deployments. The personal identifier is the name.

6.3   What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?
EPA-70

6.4   <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

Low (minimal) to none. The risk is low/minimal due to the access control levels used by the application. User rights, permissions, and group associations are in place. Access control to user records is governed by user rights, permissions, and security group membership, which is managed by the OEM System Manager and EMP Help Desk after authentication and account validation via the Agency's Enterprise Web Access Management system. Only Supervisors and Data Managers (i.e. Removal & SHEM), and Coordinators (i.e. RSC & Training) have access to the Personal and Emergency Contact information.

<u>Mitigation</u>:

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.

*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, 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, MC 2831T, 1200 Pennsylvania Avenue, NW., Washington, DC 20460.

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 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

Low (minimal) to none. Usage information is clearly stated on the portal page in the system containing the data.

<u>Mitigation</u>:

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?

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 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 40 CFR Part 16.

8.3   How does the system notify individuals about the procedures for correcting their 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 40 CFR Part 16.

8.4   <u>Privacy Impact Analysis</u>: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

<u>Privacy Risk</u>:

Low to none. There is nothing that prevents a user from correcting their data.

<u>Mitigation</u>:

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.