

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: Multi-Regional UIC Database	
Preparer: Richard Hall	Office: R4/EPA/Water Division/Clean Water Branch/UIC
Date: 2-3-21	Phone: 404-562-8067
Reason for Submittal: New PIA <input checked="" type="checkbox"/> Revised PIA <input type="checkbox"/> Annual Review <input type="checkbox"/> Rescindment <input type="checkbox"/>	
This system is in the following life cycle stage(s):	
Definition <input type="checkbox"/> Development/Acquisition <input checked="" type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input 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:

The system is a database and user interface designed to facilitate work in EPA UIC (Underground Injection Control) programs. The primary function is to track authorizations (permits, exemptions, etc) and injection wells associated with those authorizations. The system will include tools for data analysis, document preparation, reporting, and review of authorizations and associated activities (enforcement, financial responsibility, ownership, facilities, site inspections, UIC personnel, etc).

This system is identical to systems already utilized and maintained separately in each region, we are simply creating a single central system that will accommodate any region that chooses to join.

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?**

Safe Drinking Water Act (42 U.S.C. § 300f)

- 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?**

We are currently working toward developing a system security plan and intend to acquire an ATO.

- 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.**

Form No.	OMB No.
7520-6	2040-0042
7520-7	2040-0042
7520-8	2040-0042
7520-11	2040-0042
7520-16	2040-0042
7520-17	2040-0214
7520-18	2040-0042
7520-19	2040-0042

- 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. We currently intend to house on an Azure server, it is FedRamp approved and a PaaS.

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).**

The names, addresses, phone numbers, and email addresses of companies or individuals associated with authorization, well, or facility ownership, operation, or financial

responsibility will be collected. The expectation is that contact information provided by individuals is business related as opposed to personal.

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

The information will be collected during authorization issuance and throughout the life of the authorization, which includes modifications, file reviews, compliance, and enforcement actions.

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.

Proper training of data entry people and periodic review of data by region specific administrators. There are additional features built into the database to check data entry.

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 that contact information stored in the database will be inaccurate.

Mitigation:

Proper training of data entry people, periodic file reviews, and periodic review of data by region specific administrators. When data has a specified format, finite number of possible values, or a value range, then dropdowns are provided and/or automated checks are implemented to ensure that incorrect information is not entered into the data tables.

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?

We implement controls on data overwriting and entry privileges. A LAN ID and password, which are issued and maintained by the Agency, are required to access the write-capable user interface.

User groups are defined to determine what type of data can be manipulated by each user, with “Users” having the capability to manipulate non-destabilizing data (destabilizing would be table keys, system generated IDs, lookup table information, etc), whereas “Admins” will be capable of manipulating all data.

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

They are documented in the Developer Manual

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

Each region will have one or more administrators that can manipulate any data in the system.

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?

UIC employees and software development contractors will have access to the writable version of the application, FAR clauses are included in the contractor 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.

As historical records have value for reference purposes, and space limitations should not be an issue, we intend to retain the database information indefinitely. The RCS number for UIC is 1047.

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:

Indefinite retention introduces the possibility that some information in the database will not be current or accurate.

Mitigation:

Periodic file reviews are conducted to ensure that authorization files are up-to-date and complete. This process involves scouring of database records for updating, entry, or deletion of appropriate data to ensure accuracy.

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 will not be shared outside of EPA as part of normal agency operations.

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

NA

- 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?**

NA

- 4.4 Does the agreement place limitations on re-dissemination?**

NA

- 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:

None. There is no external sharing.

Mitigation:

NA

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 only contains UIC data, only tracks UIC workflows, and every tool is related to

facilitating UIC work. The system doesn't include capabilities that make it useful for anything else.

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

The yearly "Information Security and Privacy Awareness Training" mandated by the Agency.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk of improper/untimely audit

Mitigation:

Periodic file reviews are conducted to ensure that authorization files are up-to-date and complete

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 primary use is to facilitate UIC work in EPA.

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.)

Different types of information are obtainable through the system based on categories that are selected using tabs. Tabs provide pools of data based on category that can be further refined by using filtering criteria.

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?

Access control policies and access enforcement mechanisms will be implemented with access control lists. Access will only be provided to those individuals with a "need to have

access”. Encrypted communication protocols will be used to transmit PII along with the use of a security token to log into the application. Annual reviews will be conducted to determine if the database will need to continue to collect and/or access PII.

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:

That individual contact information will be obtained for purposes other than UIC regulation.

Mitigation:

The data can only be accessed by authorized users that enter a LAN ID and password. Users are categorized into groups based on the type of work that they do, and PII is only accessible by individuals for which access would be appropriate.

***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: