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 Roster.docx

System Name: Integrated Compliance Information System		**System Owner:** Jeffrey Clark	
Preparer: Emmanuel Wood		**Office:** OECA/OC	
Date: 09/27/2024		**Phone:** (202)564-3174	
Reason for Submittal:			
New: ☐	Revised:☐	Annual Review: ☒	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: ☒	Rescindment/Decommission: ☐		

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:

The purpose of ICIS is to meet the information management needs of OECA's enforcement and compliance program; the needs of the Clean Water Act's NPDES permitting, enforcement and compliance program; and the needs of the Clean Air Act's stationary source enforcement and compliance program. Current and anticipated users of ICIS include OECA, the Office of Water (OW), the Office of Air and Radiation (OAR), EPA regions, states authorized to implement the NPDES program, and states and localities authorized to implement Title V of the Clean Air Act regarding stationary sources. Some entities regulated under the NPDES program submit data to ICIS using ICIS's electronic reporting tools. ICIS provides the central source of compliance and civil enforcement data and processing for OECA.

Section 1. 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?

ICIS supports the information management needs of OECA's enforcement and compliance program; the needs of the Clean Water Act's National Pollutant Discharge Elimination System (NPDES) (40 CFR Part 122) permitting, enforcement and compliance program; and the needs of the Clean Air Act's (Section 112) stationary source enforcement and compliance program (Section 112 and 40 CFR Parts 60, 61, 63). Current and anticipated users of ICIS include OECA, the Office of Water (OW), the Office of Air and Radiation (OAR), EPA regions, states authorized to implement the NPDES program, and states and localities authorized to implement Title V of the Clean Air Act regarding stationary sources. Some entities regulated under the NPDES program submit data to ICIS using ICIS's electronic reporting tools. The NPDES eReporting Rule was promulgated in 2016 and requires the electronic submissions of data, which ICIS supports. ICIS also supports Goal 5 (Protecting Human Health and the Environment by Enforcing Laws and Assuring Compliance) of the EPA Strategic Plan that covers authority activity for all statues.

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, a system security plan has been completed for ICIS.

Current ATO expires on March 18, 2025

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?

No, ICIS data does not use cloud storage. ICIS Data is stored at NCC (RTP).

Section 2. 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).

EPA Regional Enforcement Action documents, Compliance Monitoring documents, Incident reports, and NPDES Permit contains the information.

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

EPA Regional Enforcement Action documents, Compliance Monitoring documents, Incident reports, and NPDES. Each Permit contains the information.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ICIS does not have commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Data review form entered by permittees is reviewed to ensure compliance with regulations. The accuracy of the data is ensured by quality assurance regular reports reviewed by the Regions and Headquarters data system administrators.

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: Finding out dates when the investigators will be on site for the inspection.

Mitigation: This risk is mitigated by the following controls:

- Access to the system is limited to trusted users that have credentials to log into ICIS.
- Accounts are assigned from EPA Headquarters or Regions.
- 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. 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?

To manage CWA NPDES Permit information and Enforcement and Compliance activities for all statutes.

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

ICIS does not use any kind of personal identifier to locate a specific individual.

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

ICIS does not support retrieval of information by a personal identifier. We use the permit number to retrieval of information.

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 developer system is maintained by Booz| Allen, a contractor who has access to this information. The Privacy Act FAR clauses are included in the 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.

NARA Disposal Authority: N1-412-05-5c

Permanent

Transfer to the National Archives after each major version change, as specified in 36 CFR 1235.44-1235.50 or standards applicable at the time.

The Records Schedule Number for ICIS is 0027.

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:

Per Records Control Schedule 0027, records are considered Permanent.

Mitigation:

Data is submitted to NARA for Archival with each major enhancement.

Section 4. 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.

ICIS does not share information outside of the agency.

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?

ICIS does not share information outside of the agency.

4.4 Does the agreement place limitations on re-dissemination?

ICIS does not share information outside of the agency.

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:

Users can only access specific information based on their user role.

Mitigation:

ICIS has logs that can trace an incorrect submission.

The incorrect submission can be corrected.

Section 5. 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?

Only verified permits are accepted. Procedure requires that individuals with the authority to update user access and roles regularly review this information.

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

Each year all users must take a course, Rules of Behavior, that covers what is addressed in this PIA. In addition, users need to successfully pass the annual Security Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

ICIS System Administrators do not follow established procedures.

Mitigation:

This information is reviewed by administrators annually.

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

To manage CWA NPDES Permit information and Enforcement and Compliance activities for all statutes.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☐ 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.

ICIS does not use any kind of personal identifier to locate a specific individual.

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.

The system is password-protected, and access is restricted to authorized individuals who have a work-related need to utilize the information in the system. Permission-level assignments allow users access only to those functions for which they are authorized. All records are maintained in secure, access-controlled areas or buildings. The system is accessed from an internet browser using the Agency's secured portal and requires a user to have an established log-in name and password.

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:

Finding out dates when the investigators will be on site for the inspection.

Mitigation:

Security controls are in place to limit access to this information. Auditing ICIS keeps logs in case it is needed.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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?

Click or tap here to enter text.

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:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.

Section 8. 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 Freedom of Information Act (FOIA).

Privacy Risk:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.