United States Environmental Protection Agency

# PRIVACY IMPACT ASSESSMENT

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

| | |
|---|---|
| **System Name: Integrated Compliance Information System** | |
| **Preparer: Wendell Wright** | **Office: OECA/OC** |
| **Date: 04/09/2018** | **Phone: 202-564-4259** |
| **Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review__Y__ Rescindment ____** | |
| **This system is in the following life cycle stage(s):** | |
| Definition ☐ Development/Acquisition ☐ Implementation ☐ | |
| Operation & Maintenance ☒ Rescindment/Decommissioned ☐ | |
| **Note: 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 goal 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. Assurances that the data are not subject to unauthorized or accidental alterations are important to ensure that accurate data are presented. To protect the data within the ICIS database, security procedures have been and continue to be designed and implemented to maintain the integrity of the data, to allow or disallow a user access to a database object in the ICIS database, to identify which user creates or changes the data, and to provide recovery of the data when necessary.

The NetDMR and NeT Tools allow members of the regulated community to submit electronic DMRs, and other information to EPA. CROMERR checklists for NetDMR and NeT have been thoroughly reviewed and vetted by EPA's Technical Review Committee (TRC) to ensure that electronic submissions from the regulated community using these tools follow OMB and NIST guidelines for Identity Proofing and Non-repudiation. NetDMR and NeT users can view, update, and submit only data associated with their permit(s) only after successfully logging into the system. Logins are tracked and displayed to the user on subsequent logins. Access to a permit is located by a nine digit.

# Section 1.0 Authorities and Other Requirements

## 1.1 What specific legal authorities and/or agreements 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?

Yes

## 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.

# 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).

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 from 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 when the investigators will be on site dates 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 user name and password each time they access the system.

## Section 3.0 Uses of the Information

*The following questions require a clear description of the system's use of information.*

### 3.1 Describe how and why the system uses the information.

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

### 3.2 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.*)

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

### 3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?

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

### 3.4 What Privacy Act System of Records Notice(s) (SORN(s) apply to the information?

ICIS does not require any SORNs.

### 3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.

Dose not applies to ICIS.

### 3.6 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 when the investigators will be on site dates for the inspection.

**Mitigation:**

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

## Section 4.0 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.*

### 4.1 How does the system provide individuals notice prior to the collection of

**information? If notice is not provided, explain why not.**

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. Permittees submit information through CDX collection. There is a Privacy Act Statement at the collection page.

### 4.2 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?

Access and use of the system is limited to authorized users who have a need to know this information without the required information the permit will not be issued **Privacy Act Statement** at the collection page**.**

### 4.3 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:** The system does not provide individuals with notice as ICIS.

**Mitigation:** No mitigation is required.

## Section 5.0 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.*

### 5.1 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?

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.

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

ICIS has four types of users. WAM has technical system users accounts (1 developers, systems engineers, and (2 database and (3 administration staff) and EPA has General EPA (4 application users with user accounts.

## 5.3 Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)? data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

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.

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

Users are granted by least need from the roles. A user will have access to their information but other users will not. The developers can code and test but not implement code. Database configures the data and queries. With least privilege with-in the database users. User accounts are established, and access to the system is password protected (unique to each user).

## 5.5 Explain how long and for what reason 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.

## 5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist? Yes

## 5.7 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 with 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 6.0 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.*

### 6.1 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 the Agency.

### 6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

N/A

### 6.3 Does the agreement place limitations on re-dissemination?

ICIS does not share information outside the Agency.

### 6.4 Describe how the system maintains a record of any disclosures outside of the Agency.

ICIS does not share information outside the Agency

### 6.5 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 the Agency

### 6.6 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?*

ICIS does not share information outside the Agency

**Privacy Risk:**

Roles are in place that users can only their own information.

**Mitigation:**

ICIS has logs that can trace an incorrect submission

The incorrect submission can be corrected

## Section 7.0 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.*

### 7.1 What are the procedures that allow individuals to access their information?

ICIS does not share information, a user can only look at permits,

### 7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Because ICIS does not contain or share personal information, no procedures are required.

### 7.3 How does the system notify individuals about the procedures for correcting their information?

All information is submitted through CDX for Verification. If invalid information is submitted, the user will get a message indicating that the information was did not processed so the permittee can resubmit.

### 7.4 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:**

Does not apply because no individual personal information is contained in the system.

**Mitigation: None**

## Section 8.0 Auditing and Accountability

*The following questions are intended to describe technical and policy based safeguards and security measures.*

### 8.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

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

### 8.2 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.

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

**Privacy Risk:**

If ICIS System Administrators do not follow established procedures.

**Mitigation:**

This information is reviewed periodically with them.