

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: Integrated Compliance Information System (ICIS) | |
| Preparer: 1. Lauren Jones 2. Cindy M. Hobus/ICIS Section Chief and System Owner | Office: OECA/CA/ETDD/ ICIS OM&M Section |
| Date: 08/20/2021 | Phone: Wendell Wright 202-564-4259 Cindy Hobus 202 564 8413 |
| Reason for Submittal: New PIA ___ Revised PIA ___ Annual Review <u>X</u> Rescindment ___ | |
| This system is in the following life cycle stage(s): | |
| Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/> | |
| Operation & Maintenance <input checked="" 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 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 Executive Order(s) permit and define the collection of information by the system in question?

ICIS supports the management needs for the Office of Enforcement and Compliance Assurance: "Pursuant to the Clean Water Act (CWA), 33 U.S.C. 1251 et. seq., the U.S. Environmental Protection Agency (EPA) is proposing the National Pollutant Discharge Elimination System (NPDES) Electronic Reporting Rule." Please let me know if you need anything more for CWA.

CAA - 42 U.S.C. §7401 et seq. (1970) - <https://www.epa.gov/laws-regulations/summary-clean-air-act>

CWA - 33 U.S.C. §1251 et seq. (1972) - <https://www.epa.gov/laws-regulations/summary-clean-water-act>

The main ICR for the NPDES program is at:

https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201902-2040-001

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?

ICIS does have an ATO. The next full assessment will be in August 2021.

- 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.**

ICIS is covered by the PRA: 44 USC §3501 et seq. (1980) (EPA ICR Number 0107.12, OMB Control Number 2060-0096)

- 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?**

Currently ICIS Data is not stored in the Cloud.

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 compliance information per section 1.1 regulations.

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

The compliance and permit data is transmitted to ICIS by regulated entities and permittees using NeTDMR, EDT, and in some cases NeT.

- 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 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:

Non authorized users access the system.

Mitigation:

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. (Access process is documented as part of WAM, CDX and CROMERR). 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.)

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?

ICIS ensures those that use the data within ICIS do so in accordance to their established roles and level of access;

The system's permission-level assignments only allow users to perform functions for which they are authorized preventing the misuse and handling of information. (Access process is documented as part of WAM, CDX and CROMERR). 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. Audit logs and scans monitor access per above.

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

CDX/CROMERR WAM procedures are documented within OMS WAM and CROMERR/CDX security procedures.

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

Other roles and responsibilities associated with the system are:

1. NCC – they ensure the ICIS environment, hardware, and operating systems are functioning and updated with current security patches; and
2. Booz Allen contractors – who perform the same functions as 1. Above except for the Development, Test, and Stage environments for ICIS.

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?

- Contractors (FAR clauses are within the contract) including NCC – see section 3.3
- Downstream consumers of data – ECHO and Envirofacts use data from the ICIS COPY data source to populate their systems
- EPA staff - for problem trouble shooting and analysis.

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 Control 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:

Due to the permanent retention of records, there is a low risk of data being lost.

Data record control is reviewed and strictly followed in accordance with NCC procedures

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.

Data within ICIS is only used within EPA.

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

Not Applicable

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?

Not Applicable

4.4 Does the agreement place limitations on re-dissemination?

Not Applicable

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? Only authorized and authenticated users are allowed access to the data within ICIS.*

Privacy Risk:

Since information is not shared outside of EPA, there is no risk associated.

Mitigation:

None

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?

To ensure that the information is used as stated in 6.1; ICIS has in place certified Rules of Behavior. Audit logs and scans monitor usage.

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

EPA Users and contractors are required to take the Annual Information Security and Awareness and Privacy training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Due to a certified rule of behavior, there is a low risk of misuse of data from its intended use described in 6.1.

Mitigation:

Use of audit reports and requiring certification of rules of behavior for ICIS mitigates risk.

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.

ICIS supports the management needs for the Office of Enforcement and Compliance Assurance: "Pursuant to the Clean Water Act (CWA), 33 U.S.C. 1251 et. seq., the U.S. Environmental Protection Agency (EPA) is proposing the National Pollutant Discharge Elimination System (NPDES) Electronic Reporting Rule."

CAA - 42 U.S.C. §7401 et seq. (1970) - <https://www.epa.gov/laws-regulations/summary-clean-air-act>

CWA - 33 U.S.C. §1251 et seq. (1972) - <https://www.epa.gov/laws-regulations/summary-clean-water-act>

The main ICR for the NPDES program is at:

https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201902-2040-001

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.)

Data is retrieved using permit and facility i.d. within ICIS.

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?

Only those with appropriate credentials can view the data. Unauthorized users would be visible on audit logs/scans.

6.4 Privacy Impact Analysis: Related to the Uses of Information

When regulated entities and permittees enter their data they are presented with a disclaimer stating they should not enter data they consider private.

Privacy Risk:

There is a very low risk that information in the system may be misused or inaccurate.

Mitigation:

In addition to access controls, the following disclaimer is provided to those entering data into the system:

EPA may make all the information submitted through this form (including all attachments) available to the public without further notice to you. Do not use this online form to submit personal information (e.g., non-business cell phone number or non-business email address), confidential

business information (CBI), or if you intend to assert a CBI claim on any of the submitted information. Pursuant to 40 CFR 2.203(a), EPA is providing you with notice that all CBI claims must be asserted at the time of submission. EPA cannot accommodate a late CBI claim to cover previously submitted information because efforts to protect the information are not administratively practicable since it may already be disclosed to the public. Although we do not foresee a need for persons to assert a claim of CBI based on the types of information requested in this form, if persons wish to assert a CBI claim we direct submitters to contact the NPDES eReporting Help Desk (NPDESeReporting@epa.gov) for further guidance.

***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:

Mitigation: