

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – 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: Enforcement and Compliance (EC)		System Owner: Dwane Young	
Preparer: Joe Carioti		Office: OFA/OCIO/ITESD	
Date: 8/4/2026		Phone: (202)-566-1214	
Reason for Submittal: Modernizing the ICIS system and new capability being implemented			
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 Enforcement and Compliance (EC) system is a modernization of the Integrated Compliance Information System's Federal Enforcement & Compliance (ICIS) capability. Enforcement and Compliance (EC) is a new system. The goal of the system is to meet OECA's and Regional Office's Enforcement and Compliance Program needs.

Integrated Compliance Information System (ICIS) is a legacy system that supports multiple businesses. The modernization will decouple the business processes and fit them to appropriate systems. This first phase is the Enforcement and Compliance capabilities - there is no requirement for other legacy ICIS capabilities to be coupled into one IT System in the future.

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?** There is not a single statute that provides OECA the authority to collect information, but it is outlined in the various environmental statutes.

Statutory Authority	Primary Regulation
Clean Air Act	40 CFR Part 68
Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA)	40 CFR Parts 150-189
Emergency Planning and Community Right-to-Know Act	40 CFR Parts 350, 355, 370
Resource Conservation and Recovery Act	40 CFR Parts 260-273
Clean Water Act (CWA) 311	40 CFR Parts 110, 112-113, 116-117, 300
Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA)	40 CFR Parts 300, 302, 304-306

- 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?**

The legacy ICIS system has a security plan and an active ATO; the new system will have its own security plan with an updated ATO once modernization is completed. The current ICIS ATO expiration date is: 2/26/2028 We are working with security through the ATT/ATO process for the new system.

- 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.**

The Enforcement and Compliance activities are exempt from PRA.

- 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, the data will be stored in the cloud, and the CSP (AWS) is FedRAMP-approved. The solution will primarily leverage PaaS services.

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).

The system collects Regional Enforcement Action documents, which contain information such as locational information, contact information, topic of interest information. The system uses data from other EPA systems so that it is not collected multiple times; for example, locational data from FRS or the Program system. Data that meets the criteria for public dissemination is made available for consumers.

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

Information is entered into the system by EPA or its representative. No, not a contractor. It is my understanding that there is a use case of: an inspector who is not an EPA employee that is EPA (inspector) credentialed. In this case they could be collecting the information and providing it to EPA.

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 commercial or public data is used.

2.4 Discuss how accuracy of the data is ensured.

From requirement discussions, the inspection report is signed off usually by the Branch Manager over the inspector.

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?

Yes. The system uses role-based access control and least-privilege principles to limit users to the information required for their assigned duties. Access to restricted or sensitive information, including Controlled Unclassified Information (CUI), requires an additional approved role or permission. Approved administrators review, monitor, and manage access.

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

Access controls are documented in the system security plan, Rules of Behavior, and applicable EPA account-management and access-control policies and procedures.

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

Yes. Assigned roles and responsibilities include the System Owner, business and data owners, system administrators, security and privacy personnel, authorized application users, and contractor support personnel. Each role is limited to the functions and information necessary to perform assigned duties.

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?

Authorized EPA employees, EPA-credentialed representatives, and authorized contractor personnel supporting system development, operation, and maintenance will have access based on their official responsibilities and approved need to know. Access to restricted or sensitive data is specifically approved by the appropriate business or data owner. Applicable Federal Acquisition Regulation privacy and security clauses are included in contracts involving system or data access.

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 needed to support EPA enforcement and compliance activities and in accordance with the applicable EPA records control schedule and any litigation hold or other legal preservation requirement. The specific records schedule number will be confirmed with the Records Liaison Officer before final approval.

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: Access to sensitive information

Mitigation: The system has Role-Based Access Control capabilities where approved administrators can review, monitor, and manage access to sensitive information.

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.

Data collected and processed in the system does eventually become public. The data is made available for consumption via other EPA systems. Currently ICIS does exchange data with FRS, envirofacts, and ECHO.

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

Public availability of information is generally **compatible with transparency** when it supports the original purposes for which the information was collected, such as accountability, oversight, and public engagement.

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?

Access to public information is available by default on downstream EPA systems (i.e., FRS, Envirofacts and ECHO); no agreements or MOUs are necessary to access that data. Access to restricted/sensitive data is need-to-know and would be reviewed by the appropriate business and data owners.

4.4 Does the agreement place limitations on re-dissemination?

No.

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:

Not applicable as the data is publicly available.

Release of sensitive information

Mitigation:

For sensitive information the system will have least privileged access implemented, meaning that by default users will not have access but access will have be explicitly granted to the information. This information will also be protected by role-based access control.

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?

The system has a Rules of Behavior.

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

There is no specific training for this system, but EPA does require annual Information Security and Privacy Awareness Training (ISPAT).

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:

Insufficient implemented technical and policy-based controls resulting in unauthorized access to sensitive information.

Mitigation:

Implement and periodically assess appropriate technical and physical safeguards including least privilege, role-based access, encryption, and audit logs.

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.

The information collected and maintained is used to oversee and run the Enforcement and Compliance Program. The data elements are used to inform enforcement business, and the outcome artifacts are provided to the respective external entity and made publicly available. Some data elements are used to assess the criticality of an event in support of the Agency mission.

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.

When a user is established in the system a GUID (globally unique identifier) will be created for that user. The guid will be linked to respective information and can uniquely identify a user.

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 requires the ability to capture data that may be determined to be Controlled Unclassified Information (CUI). These data fields will have an additional role/permission that the user must possess to gain access to the information – least privilege. The information can be obtained directly by EPA or provided by the external entity. For example, when an EPA Inspector conducts an inspection, they may take a picture of a proprietary business process which could be considered CUI and not made publicly available. You enforced Role-based Access controls, so that access is limited.

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:

Releasing or accessing sensitive information

Mitigation:

The system will have role-based access control (RBAC) along with logging/auditing of access to sensitive information.

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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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. 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:

Mitigation:

I attest as the Agency Privacy Officer that **Enforcement and Compliance (EC)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt. Branch
EPA/OFA

**ROBERT
KELLY**

Digitally signed by
ROBERT KELLY

Date: 2026.09.28
10:31:14 -04'00'