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%20Roster.docx

System Name: Enforcement and Compliance History Online (ECHO)	
Preparer: John Veresh	**Office:** OECA/OC
Date: 01/03/2024	**Phone:** 202.564.2509
Reason for Submittal: New PIA____ Revised PIA__ __ Annual Review__X__ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **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:

Enforcement and Compliance History Online (ECHO) is a web tool developed and maintained by EPA's Office of Enforcement and Compliance Assurance for public use. The ECHO website provides environmental regulatory compliance and enforcement information for over one million regulated facilities nationwide. It also offers information about compliance and enforcement activities at the state level.

The ECHO website includes environmental permit, inspection, violation, enforcement action, and penalty information about EPA-regulated facilities. This facility information generally covers four major environmental statutes over the past five years. Facilities included on the site are Clean Air Act (CAA) stationary sources; Clean Water Act (CWA) facilities with direct discharge permits, under the National Pollutant Discharge Elimination System; generators and handlers of hazardous waste, regulated under the

Resource Conservation and Recovery Act (RCRA); and public drinking water systems, regulated under the Safe Drinking Water Act (SDWA). ECHO also includes information about EPA cases under other environmental statutes. When available, information is provided on surrounding demographics, and ECHO includes other EPA environmental data sets to provide additional context for analyses, such as Toxics Release Inventory data. In addition, aggregate data on compliance and enforcement activities by state are provided in the State Comparative Maps and Dashboards features.

ECHO makes the data accessible online in an understandable and searchable format, with data from these systems provided in a comprehensive and organized way. ECHO also allows users to sort and analyze data in many ways, according to their needs. The public can monitor environmental compliance in communities, corporations can monitor compliance across facilities they own, investors can more easily factor environmental performance into decisions, and more.

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?

Most of the data in ECHO consists of data from other EPA data systems. Therefore, legal authorities or Executive Orders pertain to the EPA data systems of record that collect the data. ECHO does collect some information from EPA staff and delegated agencies, authorized by the following statutes:

Clean Air Act 42 U.S.C. §§ 7414(a)(2), 7414(c), 7542(b), 7525(c); Clean Water Act 33 U.S.C. §§ 1318(a) 1318(c); Comprehensive Environmental Response, Compensation, and Liability Act 42 U.S.C. §§ 9604(d) 9604(e), Executive Order 12580, section 2(j)(2); Emergency Planning and Community Right to Know Act; Federal Insecticide, Fungicide, and Rodenticide Act 7 U.S.C. §§ 136f(b), 136g, 136u, 136w-1; Resource Conservation and Recovery Act 42 U.S.C. §§ 6927(a); Safe Drinking Water Act 42 U.S.C. §§ 300j-4(b)(1); Toxic Substances Control Act 15 U.S.C. §§ 2610(a); Oil Pollution Prevention and Response; Non-Transportation-Related Onshore and Offshore Facilities; Final Rule 33 U.S.C. §§ 1321(m)(2)(B)

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?

ECHO has a System Security Plan which is maintained in Xacta. ECHO has an Authorization to Operate as a FISMA Moderate application, which expires on April 25, 2026.

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 Information Collection Request (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?

Yes, some of ECHO's data will be stored in EPA's Amazon Web Services (AWS) hosting environment, which is FedRamp approved. ECHO will use AWS' PaaS offerings to provision servers.

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).

ECHO collects limited user information to allow public and government access to certain tools. ECHO stores the emails and EPA user IDs of users that log into ECHO using Login.gov user authentication. ECHO also stores the names and states of external users who log in with EPA accounts, and of EPA users.

ECHO includes the following tools where users can enter data:

- Document Upload tool
- State Review Framework (SRF) Data Verification
- ECHO Notify,
- Error Reporting, and
- Report Environmental Violations.

ECHO's document upload tool allows users to attach documents related to enforcement and compliance actions for specific facilities. The document upload feature on the Detailed Facility report is only accessible to EPA users, and only allows the user to upload PDF files, the content of which are not recorded. The document upload tool collects the LAN ID of the user who uploaded the file. It does not collect PII data elements.

The SRF Data Verification Tool supports the annual data verification process, which helps ensure that the rests on a solid foundation of quality data. The Data Verification Tool is available to EPA and state/local environmental agencies. The Data Verification allows users to select files and save or "flag" them for review under their individual user accounts. It does not collect PII data elements.

ECHO Notify allows users, authenticated through Login.gov, to receive weekly email notifications that identify changes to enforcement and compliance data in ECHO for various environmental programs. Notifications are tailored based on the geographic locations or facility IDs of interest and the notification options that are selected by each user. ECHO Notify collects user email addresses only.

The Report Environmental Violations page is used to report possible violations of environmental laws and regulations. Information submitted in the form is forwarded to EPA environmental enforcement personnel or to the appropriate regulatory authority. The system collects information from the Report Environmental Violations form, including information on suspected violators, which may include names of individuals or businesses/facilities, as well as their address, city, state, and zip code.

ECHO presents data as reported to the original source databases. The following data elements are only available to ECHO government users:

- The Industrial Stormwater Facility Search displays the name, street address, city, state, and zip code of the owner/operator of the facility. It allows users to search for facilities based on the street address, city, state, and zip code of the facility's owner/operator. These data come from the ICIS National Pollutant Discharge Elimination System (ICIS-NPDES).

- The Enforcement Case Reports display first and last names of defendants, and related business entities. The defendant is the name(s) of the facilities that were the subject of the action.
    - The Civil Enforcement Case Report displays the name and phone number of case attorneys and contacts. This information is restricted to users with enforcement sensitive access.
    - The Criminal Enforcement Case Report displays the name and role of the defendants of concluded cases.
- The Corporate Compliance Screener displays the first and last names of enforcement case defendants.

The data for the Enforcement Case Report and the Corporate Compliance Screener are sourced from the Integrated Compliance Information System (ICIS) Federal Enforcement and Compliance (FE&C) database and Summary of Criminal Prosecutions database.

ECHO website activity/usage is monitored and stored in web server logs. This information includes source IP addresses, EPA user IDs of logged in users, referrer URLs, and user agent identifiers, and is stored in EPA's National Computer Center data center for 3 years.

Error Reporting data is tracked for troubleshooting purposes and only available to ECHO administrators.

ECHO displays names and email addresses of key EPA and state agency contacts within the website to coordinate data quality initiatives and route questions from users. This information is available only to government users that log into ECHO. Public users are directed to a contact form (which is a separate EPA webpage outside of the ECHO website).

ECHO also plans to launch in 2024 public and government only portals for Methane Super-emitter Program and will store contact information for that program to send email notifications to companies about reported methane leaks. Those company email addresses will be stored in our database but will not be searchable by personal identifier in ECHO.

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

The enforcement and compliance data are copied from other EPA program systems. However, some limited information is collected directly from users and is described in section 2.1. A list of ECHO source systems can be found at: ~~https://echo.epa.gov/resources/echo-data/about-the-data#sources~~ https://echo.epa.gov/resources/echo-data/about-the-data

The only PII collected by ECHO are the email address and display name for EPA, State, other government, and public users, which are received from EIAM or login.gov and stored in our MySQL database on the web server.

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

ECHO does not use information from commercial sources. ECHO displays data from EPA program data sets, which are publicly available.

2.4 Discuss how accuracy of the data is ensured.

The compliance and enforcement data collected are suitable for public release, per review processes

established by program offices. ECHO follows a quality assurance plan and additionally, the ECHO web application includes integrated error correction, which allows the public to submit error reports about information displayed in ECHO to EPA. Error reports are routed to FRS's Error Tracking System (ETS), which then manages correspondence between EPA and state data stewards, who are responsible for evaluating and addressing them.

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 potential risk in displaying inaccurate data to users from EPA source systems that defendants or owner/operators may be mis-identified. There is low potential risk of inaccurate email contact information for users that voluntarily sign up to use ECHO Notify that wish to be notified of changes to data.

Mitigation:

Users cannot search using PII about individuals on ECHO, but they may see names in reports for one facility at a time. The public can report potential data inaccuracies through EPA's integrated error correction system. Error reports may be submitted to EPA, who will evaluate and address the reports. ECHO users can verify their own email address on the ECHO Notify page, and update contact information through Login.gov.

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?

ECHO uses multiple access levels to control access to data and site features. Public-facing access levels are: public, government, EPA, and enforcement sensitive. Internal administrative access levels are: author, editor, developer, app administrator, database administrator, web administrator.

Access levels are implemented by Web Application Access communities (aka WAM groups). For example, to view government-only content, a user must apply through EPA's Web Application Access application to join the ECHO Government Users community. ECHO staff verify that the user is a government employee or contractor, and if so they approve the request. Membership in ECHO Government Users then enables the user to see government-only data and features in ECHO.

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

ECHO follows EPA Access Control Procedures CIO 2150-P.01.2.

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

No. See the description in section 3.1.

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?

ECHO classifies its information into multiple categories by the required level of access, as shown in the following table.

Category	Description/Examples	Who Can Access
Public	• ECHO Notify • All other data not categorized as government, EPA, enforcement sensitive, or ECHO staff	Anyone
Government	• SRF Data Verification Tool • Inspection and enforcement targeting tools	Employees of US state, local, tribal, and Federal government agencies and their contractors
EPA	• Enforcement and compliance documents • Environmental justice dashboards • Lead maps	EPA employees and contractors
Enforcement sensitive	• Enforcement cases referred but not yet public	EPA employees and contractors who have signed enforcement access agreements and ECHO rules of behavior
ECHO staff	• User email addresses, IDs, states, and dates last logged in	ECHO team (EPA employees and contractors)

EPA contractors who have access to ECHO data have the appropriate clauses in their contract. EPA requests access for their contractors as needed based on the scope of work in each 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.

Enforcement and compliance records must be retained by the system of record for 5 to 20 years, depending on whether the inspection resulted in an enforcement action. These records are covered under EPA records schedule number 1044 (Compliance and Enforcement). ECHO contains a copy of these records.

ECHO's web content, site management reports and procedures, and server logs are covered by EPA records schedule 0095 (Web sites). They must be retained for 3 to 5 years.

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: No sensitive PII will be collected so risk of privacy of individuals is limited.

Mitigation Risk: As discussed above, no sensitive PII will be collected and only ECHO staff may access user information.

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.

ECHO is a public website which includes publicly releasable PII information contained therein. No sensitive PII information is collected and no information sharing agreements are planned or in place.

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?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

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:

No information sharing agreements are planned or in place.

Mitigation:

No information sharing agreements are planned or in place.

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?

Privacy is assessed before making information available in ECHO, and ECHO help documentation is available online to accurately describe the data element, source, and use and limitations, as appropriate. Acceptable use of ECHO data is providing in writing on https://echo.epa.gov/resources/echo-data/about-the-data#use.

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

EPA provides annual Security and Privacy Awareness training to all EPA staff and contractors. Privacy notices are displayed in the footer of all ECHO pages. PII is provided voluntarily by users of ECHO Notify and EPA communicates in writing (on https://echo.epa.gov/tools/echo-notify) how that information will be used. The ECHO product owner, security officer, lead architect, and all developers take EPA Role-Based Training annually as required by EPA policy.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is low risk of PII being released or shared outside of the intended users.

Mitigation:

Review processes established by program offices for the source systems help mitigate 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.

The ECHO website provides publicly available environmental regulatory compliance and enforcement information for over one million regulated facilities nationwide. It also offers information about compliance and enforcement activities at the state level. The ECHO website includes environmental permit, inspection, violation, enforcement action, and penalty information about EPA-regulated facilities.

With the understanding that business contact information is not PII, the only PII that ECHO uses are the username and email addresses of ECHO users, which it receives when user's login via EPA single-sign on or login.gov. ECHO stores that information to track site usage and troubleshoot access issues.

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.)

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 ECHO team follows all of the necessary administrative and technical controls identified in the appropriate agency policies, procedures and guidance required to evaluate and ensure PII is managed properly including CIO 2150.5, Information Security Policy and CIO 2150-P.01.2 EPA Access Control Procedure.

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:

There is low risk of PII being released or shared outside of authorized users. ECHO does not include any sensitive PII.

Mitigation:

Access controls restrict access to PII to authorized users. The controls are tested as part of release testing of each production deployment.

*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.

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 8.0 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?

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 FOIA.

Privacy Risk:

Mitigation: