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: Combined Air Emissions Reporting System (CAERS)	**System Owner: Julia Gamas**
Preparer: Julia Gamas, Kevin Brundage	**Office: OAR-OAQPS-AQAD-EIAG**
Date: 10/14/2021	**Phone: 919-541-7915**
Reason for Submittal: New PIA__X__ Revised PIA__ Annual Review_____	
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:

Currently, various state, local, tribal (SLT) and federal programs require industry to report air pollutant emissions to separate U.S. EPA and SLT systems at different times of the year. This leads to redundancy and reporting burden for both industry and government. Through CAERS air emissions reporting will be streamlined for facility reporters, SLT authorities, and EPA staff. CAERS is a consolidated reporting system process for regulated entities to provide the latest facility attributes, emissions estimation input data, and shared facility and

emissions data only once.

There are four major federal reporting programs and systems of data entry:

a) National Emissions Inventory (NEI). Facility reporters send criteria emissions reports to their SLTs, and after a review and quality assurance of the data, the SLTs send it to EPA via the Emissions Inventory System (EIS)

b) Toxics Release Inventory. Facility reporters report their toxics emissions for all media to the program via TRI-MEweb.

c) Test data from facilities to comply with different industry and technology regulations are submitted via the Compliance and Emissions Data Reporting Interface (CEDRI)

d) Greenhouse Gas Reporting Program. Facility reporters report their greenhouse gas emissions through the Electronic Greenhouse Gas Reporting Tool (E-GGRT).

In the first phase of CAERS V3 includes NEI reporting with the ability for the facility to share reported data with TRI. Subscribed SLTs will be able to have their facilities report directly to CAERS, then have the SLTs review their NEI report. TRI data entered into CAERS will be added and left for pick up by TRI-MEweb, for facilities to use optionally in their TRI reporting.

Data collected in CAERS includes:

1. Facility inventory data
2. Emissions data associated with facility and sub-facility components.
3. Contact information (PII) for facility reporters and certifiers (POCs) will be collected as well. This data include: name of the reporter and/or certifier, work address, work phone number, work email address, area of expertise of the individual (e.g. emissions inventory expert).

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?

- The Air Emissions Reporting Rule (AERR), Legal Authorities: 23 U.S.C. §101; 42 U.S.C. §7401 -7671q; in 40 CFR, Part 51) requires state and local agencies to report emissions annually, including some low risk personal identification information (PII). The primary collection system for the AERR is the Emissions Inventory System (EIS), and CAERS is a system that provides a connection among facilities, state/local/tribal authorities, and EIS (among other systems).
- The Toxic Chemical Release Reporting: Community Right to Know rule (Legal Authorities: 42 U.S.C. §11023; 42 U.S.C. §11048; in 40 CFR, Part 372) requires companies that release pollutants to the environment to report annually, including some PII. The primary collection system for this rule is TRI-MEweb, and CAERS facilitates collection of that same data to provide for use by TRI-MEweb to pre-populate their data collection system. In addition to federal rules, CAERS is implementing the requirements of some state/local agencies, who are using CAERS to collect data from the facilities in their jurisdictions. As such, the state and local regulations are relevant and provide those agencies the authorities to collect data through CAERS (Legal Authorities 42 U.S.C. §7401 -7671q). These are:
    - Georgia Rules for Air Quality Control 391-3-1-.02(6)(a)4.
    - Washington D.C., Title 20, Chapter 3
    - Arizona Administrative Code, Title 18, Chapter 2, Section 327 (R18-2-327)
    - Nebraska Title 129 of the Nebraska Administrative Code
    - Rhode Island Air Pollution control Regulation 14, section 14.2.1

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?

As a program service under the Central Data Exchange (CDX), CAERS is covered by the CDX security plan. The ATO for CDX expires on August 12, 2024.

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.

a) Some data being provided from facilities to the EPA is covered by the TRI program Information Collection Request (ICR): OMB control number: 2070-0212.

b) The information being provided from the states/locals/tribes to the EIS is covered under the ICR for the AERR: OMB control number 2060-0580.
c) The information being collected by the states/locals via CAERS is covered by their state/local requirements for Information Collection Requests.

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?

The data is being maintained in a Cloud. The cloud service provider is Microsoft Azure provided through CDX. The CSP is FedRamp approved. We are currently using IaaS (Infrastructure as a Service).

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).

1. Industry reporter information:
    - Name
    - Role: preparer or certifier
    - Work address
    - Work email address
    - Work phone number
    - Facility they are associated with as prepare and/or certifier
2. SLT Reviewer information:
    - Name
    - Email address
3. Facility configuration and emission data. This data is the subject of the regulation requiring the facility preparers and certifiers to enter and submit it for review by the SLT and EPA staff as indicated by the rules.

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

Preparers, certifiers and SLTs reviewers enter the information directly in the process of registering in CDX. This is low sensitive consumer PII.

2.3 Does the system use information from commercial sources or

publicly available data? If so, explain why and how this information is used.

Yes. While the facility preparers, certifiers, and reviewers, enter their contact information into CDX, which then makes its way to CAERS, their contact information may also be available in company and SLT authority websites.

2.4 Discuss how accuracy of the data is ensured.

For preparer and certifier contact information, the SLT can check that the user is associated to the correct facility via information from the permit and from the company that owns the facility.

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:

Low risk.

The primary risk to the characterization of the data is human error, which could result in the collection of inaccurate data. The information itself is categorized low risk because only limited PII is collected.

Mitigation:

As mitigation, the system avoids the collection of unnecessary data and does not capture any sensitive information. In addition, the data quality checks implemented in the system mitigate the risk of inaccurate data.

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?

Yes.

- The industry preparers and certifiers are only given access to their data via CDX registration. The SLT verifies that in the CAERS app the preparer/certifier cannot access the wrong facility by mistake.
- Only authorized preparers/certifiers can work on their designated facility report.

- Only authorized SLT authorities can review reports submitted by facilities in their jurisdiction.
- EPA staff/contractor verify that only authorized SLT reviewers are accessing CAERS before allowing them access.

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

These procedures are documented in the Common Air Emissions Reporting System User's Guide located in the CAER document library on the CAER website.

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

No other components are assigned within the system.

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?

Limited EPA staff and contractors have access to the data. The contractors that access the CAERS system are covered by relevant clauses identified in the Agency's cyber security check-list and/or by the Rights in Data clause (FAR 52.227-14).

The Combined Air Emissions Reporting System application is public-facing. Customers with password protected accounts have access to the information they have entered voluntarily and that other users have shared with them.

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.

After the facility inventory and emissions inventory records contained within the Common Air Emissions Reporting System are approved by the state, local, tribal authority they have routine operational value and are not considered essential for the ongoing management of the program or project. Therefore, these records fall under the EPA Records Schedule 1035, Item C: Routine environmental program and project records and will be stored for a minimum of ten 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:

Low. There is a risk that some records will be maintained longer than necessary.

Mitigation:

The record control schedule will be reviewed on an annual basis to ensure they are followed.

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.

Facility data and facility POC information reported by preparers and certifiers is shared with their respective SLT authority reviewers only.

Preparers and certifiers can only view data for the facilities they are authorized to enter data for. TRI emissions data is not made public while in CAERS. Once data has been moved to TRI-MEweb on a voluntary basis, and EIS, data is further reviewed by the relevant EPA staff. Only data that has undergone EPA staff review (in consultation with the SLT in the case of NEI, and in consultation with the relevant facility reporters in the case of TRI), is made publicly available in the NEI and TRI websites per the relevant air quality regulations. Data that is not required to be disclosed to each system is retained in CAERS.

EPA staff do not share any SLT point of contact information with unauthorized outside parties.

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

Because the SLT is the delegated authority for NEI data, the SLT has to be able to communicate with the industry POC's for each facility. The SLT must have access to this POC data so the SLT knows who to reach out to with questions about the report such as to request corrections in the report. Without the ability to reach out and communicate with the facility POC's the SLT cannot provide assistance to the POCs, alert them of program changes and how they should be addressed to fulfill the reporting requirements, and request corrections of the report. The SLT would thus, not be able to meet its own reporting requirement under the NEI rule.

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?

CAERS has in place an MOU with the SLT reviewer that states that any PII data they obtain from CAERS is to be used for the purposes outlined in 4.2 above, and that any other use of the data constitutes a misuse.

4.4 Does the agreement place limitations on re-dissemination?

Yes. The SLT cannot re-distribute the POC data or use it for any other purpose than to contact the POCs in regards to their reports.

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:

Risks associated with the PII data in CAERS include:

1. PII data being disclosed via a breach in the system.
2. An SLT obtaining data from another SLT
3. An SLT subsequently sharing PII data with third parties.

Mitigation:

Mitigation for the listed risks is as follows:

1. CAERS is within CDX and any PII is protected, thus, by CDX security.
2. SLT roles in CDX are limited. The SLT has some administrative abilities to work with the facility data as necessary for them to perform their duties as delegated authority. However, the SLT will *not* have Registration Maintenance Access Management (RMANS) roles. The list of POCs that each SLT can see and use in CAERS is confined to those facility reporters and certifiers who report to that SLT. One SLT cannot obtain another SLT's PII data.
3. The MOU assists in ensuring the SLT is fully aware that data sharing is not allowed, and that any PII data should only be used for the intended purposes described above (section 4.2). Furthermore, the ability for the SLT to send emails to their POCs directly from within the CAERS application, reduces the possibility that the SLT will share that list of POCs inadvertently.

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?

The system ensures the information is used as stated in Section 6.1. by not allowing facility users to access data for other facilities, and by not allowing SLT users to access data for facilities that are not in their jurisdiction.

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

EPA staff and contractors are required to take Information Security Awareness Training every year. SLT users and facility preparers and certifiers undergo training on the registration process so they understand how and why the system requires an identity verification process.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low. There is a risk that data could be accessed or modified by authorized and non-authorized users.

Mitigation:

Auditing controls are in place to monitor who is accessing and/or modifying the data in the databases. Additionally, access controls are in place to restrict un-authorized access to the data.

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.

Facility PII (contact information) is used only by the SLT to whom facilities report their air emissions, for outreach throughout the review/reporting process. E.g. to send email reminders to facility POCs about approaching deadlines, or to reach out to them with questions about their emissions report.

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.)

Users authenticate based on CDX credentials but the data they see is retrieved based on facility IDs and report IDs, not based on personal identifiers

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?

Ensuring that access to the internal applications is restricted; no public users can access the internal administrative functions ensures that the information is handled and used accordingly. The entry into the internal applications is via assigned username and password.

Additionally, the majority of information is contact information for businesses (not individuals), and the scope of information has been limited only to that data which is necessary. Limiting the amount of data collected mitigates possible risk to people with information in the system.

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:

Low risk.
Risk of an inappropriate use of data is low, because, even if the SLT were to inadvertently publish its list of POC's, it would only be disclosing information that is already public.

Mitigation:

The risk is mitigated by the implementation of access controls to limit access to specific users with a legitimate need to access the data for its intended purpose. In addition, the Common Air Emissions Reporting System User's Guide details how data should be submitted and reviewed, which mitigates this risk by ensuring that accurate information is entered. Al users must be identified and authenticated before accessing CAERS.

***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: