

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: Clean Air Markets Division Business Systems (CAMDBS)	System Owner: Paula L. Branch
Preparer: Paula L. Branch	Office: Office of Air and Radiation/Office of Air Programs/Clean Air Markets Division
Date: August 5, 2020	Phone: (202) 343-9168
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"/>	
<p>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>.</p> <p>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>.</p>	

Provide a general description/overview and purpose of the system:

This Privacy Impact Analysis documents the CAMDBS applications and addresses the privacy risks and mitigation.

The Clean Air Markets Division Business System (CAMDBS) is an Internet-based portal that supports the operation of the emissions trading programs implemented by EPA. The CAMDBS consists of five applications to achieve its mission:

- CAMD Business System (CBS)
- Emissions Collection and Monitoring Plan System (ECMPS)

- Air Markets Program Data (AMPD)
- CAMD System Administrator (CSA)
- Field Audit Checking Tool (FACT)

The CAMD Business System (CBS) is the web application used by EPA and industry to submit required program information. Users can register new facilities and submit required facility, unit, representative, agent, owner/operator, and associated data for CAMD supported programs. Users can buy or sell allowances to cover annual or seasonal emissions, transfer allowances between user accounts, bid in the annual Acid Rain auction, and conduct annual reconciliation of emissions and allowances, from which compliance is determined.

The Emissions Collection and Monitoring Plan System (EMPS) is an application to receive, process, and quality assure emissions data and monitoring plans. Users can quality assure hourly emissions data and then, via the internet, submit the quarterly emissions files.

Air Markets Program Data (AMPD) provides access to selected CAMDBS data in the CAMDBS data warehouse. Any business data reported to EPA is displayed in the AMPD web-based application. Users may retrieve emissions, deposition, allowance, and inventory data. Access to AMPD data is read-only.

The CAMD system administrator application (CSA) is a client-server tool that provides desktop access to the CAMDBS database to perform a variety of system administration functions.

The Field Audit Checking Tool (FACT) was developed to enhance Part 75 continuous emission monitoring system (CEMS) field audits.

Users must be recognized as a designated representative (primary or alternate) or an agent of a designated representative in the CAMD database to submit data to EPA using CBS or ECMPS. To have the responsibility as a designated representative, an established user can use CBS, or submit the paper Certificate of Representation form. To become an agent, you can use CBS Manage Agents module or submit the paper Agent Delegation form. Once recognized as either a designated representative or an agent in the system, a user account is created, and the user can register to use CBS and ECMPS on-line.

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?

42 U.S.C. § 7401- Acid Rain Program (ARP)

42 U.S.C. §7410 and 42 U.S.C. §7601 - Cross State Air Pollution Rule (CSAPR)

42 U.S.C. § 7412(n)(1)(A) - Mercury and Air Toxics Standards (MATS)

18 U.S.C 1001 - Standards of Performance for Greenhouse Gas Emissions for Electric Generating Units (NSPS4T)

- 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?**

Yes.

ATO expires 08/20/2021.

- 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.**

OMB No. 2060-0258

OMB No. 2060-0667

- 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?**

No.

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).**

Name

Business Address

Business Phone

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

Data is submitted primarily by regulated facilities, through a designated representative or alternate designated presentative. Agents, who act on behalf of the representatives can also submit data. Regulated facilities submit information on facility attributes, monitoring attributes, and hourly emission data. Information on allowance transfers is also submitted. The facility and allowance data is collected via the CAMD Business System (CBS). The emissions, quality assurance and monitoring plan information is collected via the Emissions Collection Monitoring Plan System (ECMPS).

- 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.

2.4 Discuss how accuracy of the data is ensured.

CAMDBS contains extensive internal controls to ensure data integrity and completeness. The system also logs all user actions and sends confirmation messages, documenting any update, to the responsible officials. All data is quality assured, validated, and verified prior to entry. Quality assurance is built into the applications with a series of tests that allow data correction. Only quality assured data is allowed submission to the CAMDBS.

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 of inaccurate data.

Mitigation:

The accuracy of the data is verified before acceptance. The ECMPS has a series of quality assurance checks that users must utilize before submission of the 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. Each user in the CAMD Business System is assigned a role. The primary roles are Administrators and Industry. Administrators have all access. Industry users have update access. As an industry user, only the individuals' information can be viewed or modified. All Industry access is limited to the information that pertains to them or the facilities for which they have responsibility

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

Access control policy and procedures documented in the System Security Plan (SSP).

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

No, there are no other components to the assigned roles and responsibilities 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?

The internal and external parties with access to the data/information in the system include:

AGENCY:
EPA CAMD
EPA Other
State/Local/Tribal

INDUSTRY:
Allowance Broker/Trader
Business Consultant
DAHS Vendor
Legal Counsel
Plant/Company Management

Contractors: Federal Acquisition Regulations (FAR) clauses are included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)

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.

The retention period and procedures for electronically reported for the CBS is delete/destroy 20 years after transfer. The electronically reported records for the CBS and ECMPS are permanent.

A record control schedule has been issued for the records in the Clean Air Markets Division Business System (CAMDBS).

Schedule #0041 Clean Air Markets Division Business System (CAMDBS).

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 Risk – Data Integrity for the large volume of data.

Mitigation:

Create an Audit Trail
Develop Process Maps for Critical Data
Eliminate Known Security Vulnerabilities
Validate Computer Systems Annually

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.**

No.

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

Not applicable, no external sharing

- 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, there are no information sharing agreements, MOUs, or other new uses of the information.

- 4.4 Does the agreement place limitations on re-dissemination?**

Not applicable, there are no agreements.

- 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:

None - No privacy risks related to information sharing.

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?**

CAMDBS contains extensive internal controls to ensure data integrity and completeness. The system also logs all user actions and sends confirmation messages, documenting any updates to the designated representatives.

The data collected by the CAMDBS relates, almost exclusively, to facility profiles and operations, as necessary for administering programs mandated by the Clean Air Act. All data to be collected is defined in the Agency's Information Collection Requests (ICR) submissions. This is subject to oversight and affected entity comment.

Auditable events are reviewed weekly by the System Owner (SO) and CAMDBS administrators. The list of auditable events within the CAMDBS system is reviewed annually, and if necessary updated, as part of the assessment process annually and when technology changes occur.

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

For EPA CAMDBS users, Information Security and Privacy Awareness Training is conducted annually. This training is mandatory and if not completed will result in system lock out.

For the regulated community, privacy training is generally provided relevant to system collection in the form of review and acknowledgement of a Rules of Behaviour form. All users must acknowledge and sign the Electronic Signature agreement detailed below:

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low Risk - Unauthorized access to PII (name)

Mitigation:

Implement Audit Procedures.

Ascertain the breach.

Disable the account.

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 Agency uses the information to determine compliance with Title V Acid Rain Program (ARP) and Title IV of the Clean Air Act Amendment of 1990. Implementation of the Cross-State Air Pollution Rule (CSAPR), Mercury Air Toxics (MATS), and NOx SIP Call, and other CAA rules.

Allowance trading allows sources in cap and trade programs to adopt the most cost-effective strategy to reduce emissions. Affected sources are required to install systems that continuously monitor emissions of SO₂, NO_x, and other related pollutants in order to track progress and ensure compliance. Sources that reduce their emissions below the number of allowances they hold may trade allowances with other sources in their system, sell them to other sources on the open market or through EPA auctions, or bank them to cover emissions in future years.

Sources regulated by the CAMD programs must follow the monitoring regulations in Part 75 of Volume 40 of the Code of Federal Regulations (CFR), which requires continuous monitoring and reporting of sulfur dioxide (SO₂), carbon dioxide (CO₂), and nitrogen oxide (NO_x) emissions.

Under the Acid Rain Program, one allowance is equivalent to 1 ton of SO₂ during a given year or any subsequent year. Under CSAPR, there are annual NO_x and SO₂ allowances, as well as seasonal NO_x allowances. At the end of each year or ozone season, the source must hold an amount of allowances at least equal to its emissions for that time period. For example, a source that emits 5,000 tons of SO₂ must hold at least 5,000 allowances that are usable in that year. Regardless of how many allowances a source holds, however, it is never entitled to exceed the limits set under Title I of the Act to protect public health.

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.)*

Information is retrieved by the Facility Identifier.

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?

CAMDBS strictly adheres to NIST 800-122 to protect the PII of name.

The non-sensitive data has been:

- Identified as residing in the system
- Minimized the use, collection, and retention
- Categorized by the PII confidentiality impact level
- Applied the appropriate safeguards based on the PII confidentiality impact level
- An Incident Response Plan has been developed to handle breaches involving PII

The CAMDBS maintains close coordination of the relevant experts helps to prevent incidents that could result in the compromise and misuse of PII.

The CAMDBS has implemented the following controls to protect the individual PII:
AP-1, AP-2, AR-1, AR-2, AR-4, AR-5, AR-6, AR-7, DI-1, DI-1(1), DI-1(2), DM-1,
DM-1(1), DM-2, DM-2(1), DM-3, DM-3(1), SE-1, SE-2, TR-3UL-1, and UL-2.

TABLE J-1: Summary of Privacy Controls by Family Id Privacy Controls is attached.

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 – Privacy risks of data availability, accuracy, and completeness

Mitigation:

Utilize system internal controls concerning data availability, accuracy, and completeness.

The CAMDBS Disaster Recovery Plan was developed in accordance with the EPA template and

- Addresses contingency roles and
- Responsibilities, assigned individuals with contact information, and
- Activities associated with restoring the system after a disruption or failure.

***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: