EPA United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Air Compliance ADI Portal (ACAP)

Preparer: Maria Malave	**Office:** Office of Enforcement and Compliance Assurance (OECA)
Date: 6/11/19	**Phone:** 202-564-7027

Reason for Submittal: New PIA__X_ Revised PIA____ Annual Review____ 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:

ACAP is an APEXLite application that will be part of the Applicability Determination Index data system. ACAP will include a public submittal portal for submittal of requests to EPA on Clean Air Act (CAA) compliance questions under the New Source Performance Standards (NSPS) and National Emissions Standards for Hazardous Air Pollutants (NESHAP) programs. ACAP public submittal portal is linked to an internal interface that addresses the process flow and recordkeeping for issuing responses to those requests. ACAP internal interface will replace the current ADI InfoManager System (AIS) internal interface. ACAP will also facilitate publication of the final EPA responses to the ADI public compliance assistance website. ACAP requires external and internal users to have a user ID and password for its use.

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?

Clean Air Act regulations under the New Source Performance Standards (40 CFR Part 60), National Emission Standards for Hazardous Air Pollutants (40 CFR Part 61 and 63), and Emission Guidelines (40 CFR Part 60), and Federal Plans Implementing Emission Guidelines (40 CFR Part 62) and Protection of Stratospheric Ozone (40 CFR Part 82)

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?

A system security plan has been drafted, but it is not yet final. The system will receive an ATO. ATO is anticipated to occur by 6/21/19.

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 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?

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).

PII for external users include:

Requestor first and last name, requestor title, and requestor mailing address, email, phone.

Authorizing Official Name, Title and email.

Facility and company physical address

Name, office phone and EPA email address of the EPA staff person assigned to respond to their request as lead staff.

Aside from PII, the system collects data about specific processes where the requestor has a question about how a regulation may apply to a process at their facility, questions about waivers or extensions to compliance dates, or questions related to alternative testing or monitoring requirements. The system also stores documents to support the request (calculations, related permits or consent decree files, or process diagrams, as well as a copy of the final signed request in a .pdf file format). The system does not accept or store any confidential business information.

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

Registered users representing affected regulated entities or state/local/tribal delegated authorities, login and submit the information in a form. The form contains information about facilities necessary to make a request for applicability determinations. Once the form is submitted, this information can be accessed by registered EPA users who will review the request and prepare a formal response, as needed. The form will be accessible using the single sign-on (SSO) LAN ID and password that a user must obtain before accessing the system. The URL for accessing the system will be https://acap.epa.gov

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.

The system does not provide extensive data validation, but instead relies on the requestor to provide accurate data as part of its request. Prior to submission, the system checks that a final signed request has been uploaded and that a select set of mandatory data fields are completed. An authorizing Official Name, Title and email is also required prior to submission to EPA.

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:

Names, email addresses, and phone numbers of external users are accessible to EPA staff using the ACAP data system. Names, email addresses, and phone numbers of EPA staff assigned to their requests are accessible to external users, but these data are already available in the EPA National employee locator, no additional data elements are made available to external users.

Mitigation:

Access to the system is limited to registered users. Users must obtain a LAN ID and password and acknowledge that they are working on an EPA data system. Additionally, there is no way for

external users to export data from the system. For internal users, while the functionality to export certain data elements from the system is being built out, those exported items will not include any PII. The exported data will be limited to information about the facility name and processes related to the specific question being asked.

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. WAM will be used to authenticate all users.

User access is determined in the USERS database table. The table includes a user name (matching the LAN ID), role, and office of the affiliated user.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

The ACAP data system follows the procedures for user access of information established in the National Institute of Standards and Technology Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations- Building Effective Assessment Plans. For external users, the ACAP data viewable will be limited to only the requests submitted under the user ID. For internal users, the ACAP data will be read-only unless the user is an administrator type user and the EPA program office has been assigned as a lead office for a request. For regular (non-administrator) users, the data will be read-only unless the user is assigned to a request as lead staff.

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

No.

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?

US EPA staff in OECA, OAQPS, and EPA Regions 1 through 10.

Contractors to USEPA staff in charge of system administration.

External users who have obtained a LAN ID with WAM that are registered to use the system. External users may include, regulated industries, state/local/tribal authorities.

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.

Records schedule 1044(a) applies. Enforcement records maintained by the Office of Enforcement and Compliance Assurance (OECA) and related to enforcement of EPA statutes, regulations and standards, including case development and litigation support files, background studies and surveillance reports, legal opinions, attorney work products, violation notices, press releases, compliance orders, and related records. There is no time limit on how long each record is retained. Currently the system is designed to store the data indefinitely. This is consistent with the setup of records retention in AIS data system and the old hard copy methods of storing copies of incoming request letters. Since ACAP will serve as a record for published EPA responses on the Applicability Determination Index (ADI), and that system goes back many decades, a limitation on records retention is not appropriate.

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:

ACAP is a new data system, it will store historical records that are transferred over from AIS, as well as new records submitted on the data entry form of the ACAP application. Records are retained indefinitely. This will include all interfaces: public submittal portal, internal interface and the public database.

Mitigation:

Access to the system is limited to registered users for the public submittal portal and the internal interface, except for the public database where there is no need for restrictions. Internal users must obtain a LAN ID and password and acknowledge that they are working on an EPA data system. External users accessing the public submittal portal also requires having a user ID and a password and can only access their request. Additionally, there is no way for external users to export data from the internal system. For internal users, while the functionality to export certain data elements from the system is being built out, those exported items will not include any PII. The exported data will be limited to information about the facility name and processes related to the specific question being asked.

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.

If a request is received that was intended for a state/local/tribal authority, the EPA may email a copy of the letter included in the request to this regulatory agency as a courtesy. However, the data submitted in the data system to EPA would not be exported to any outside party.

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

Currently the approach for making requests is entirely handled with emails and hard copy mailings. This sharing exists under the current applicability determination process and would continue once ACAP is deployed.

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?

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:

Risk is that phone, mailing address, or email and contact name for facility would be made accessible to a 3rd party source.

Mitigation:

Only documents related to the request are shared via email, at the discretion of the EPA lead staff assigned to the request. No access to the EPA internal data system is allowed for external parties.

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 in accordance with stated practices in this PIA?

The ACAP system was designed to streamline the EPA process for receiving and responding to CAA requests (ADs) and also provide more consistent responses to similar requests in different parts of the country.
The OECA compliance assistance program provides guidance to users on the AD response and publication process in the 1999 guidance manual on "How to Review and Issue CAA Applicability Determinations and Alternative Monitoring." In addition, ACAP will also be link to a compliance assistance page that will explained the AD process to external users.

ACAP does not do anything with the PII other than forwarding it to the lead subject matter expert assigned to respond to the request. When a request has been assigned to a lead staff, the requestor will receive a notification that indicates the lead staff contact information addressing the EPA response. The lead staff would need to follow the internal procedures established in the Tiering and Consultation Plan.

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

All EPA users are required to participate in Security and Privacy Awareness Training annually.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: Risk is that a user assigned to develop a response may edit a record incorrectly.

Mitigation: Internal and external user agreements for accessing EPA data systems are required before accessing the system. In addition, controls are placed on what type of data is read-only vs. read-write access.

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 ACAP data system uses information provided by external users through the public submittal portal to allow EPA to triage and assign requests to the appropriate program office and staff to respond to requests. After EPA issues a final response to a requestor, we may publish the final response to the ADI public website that provides compliance assistance to the pubic user.

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.)*

The request ID is the master number to track each request submitted through the system. Users will normally look up the data by this ID. However, summary table views also include the name of the EPA staff assigned to respond to the request and a user can sort the table by EPA lead staff name to identify the list of requests assigned to each lead staff person. Each EPA staff name is linked to an email and phone number using the EPA National Employee locator.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

None

6.4 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>: Low – EPA staff name only used to retrieve records and this data is already publicly available.

<u>Mitigation</u>: Internal and external user agreements for accessing EPA data systems are required before accessing the system.

*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 How does the system notify individuals about the procedures for correcting their information?

8.4 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: