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.

System Name: Applicability Determination Index (ADI) InfoManager System (AIS)	
Preparer: Maria Malave	**Office:** Office of Enforcement and Compliance Assurance
Date: 1/15/2020	**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:

The ADI InfoManager System, also known as AIS, is an Intranet application which provides an electronic means for receiving EPA-issued Clean Air Act applicability determination information (AD records), processing the determinations, and preparing the determinations for publication on the Applicability Determination Index (ADI) public database and a Federal Register Notice. AIS consists of a Web interface and a database. The servers which will host ADI and AIS are housed at the EPA's National Computer Center (NCC) in Durham, NC. The AD records include key data, including:

system generated control number; header and rule information (title, subparts, citations, EPA contact name and phone number, etc.); copy of the incoming request; supporting documents (e.g., performance test data); PDF of the signed letter or memoranda; abstract; and status categories to track process. The AIS URL is https://ais.epa.gov/ .

Section 1.0 Authorities and Other Requirements

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, USC 7411), National Emission Standards for Hazardous Air Pollutants (40 CFR Part 61 and 63, USC 7412), and Emission Guidelines (40 CFR Part 60), and Federal Plans Implementing Emission Guidelines (40 CFR Part 62, 7413) and Protection of Stratospheric Ozone (40 CFR Part 82, 7671).

1.1 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 ADI-AIS system security plan is being updated. The system is expected to receive an ATO before April 30, 2020, when AIS ATO expires.

1.2 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 is required.

1.3 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).

ADI/AIS collects, uses, disseminates, and maintains the following information:

- Requestor/Authorizing Official Name
- Name, office phone and EPA email address of the EPA staff person leading the response and the name of the EPA official that signed the determination letter.

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

The formal requests received from the regulated community, delegated states, locals and tribes by mail or email (with a PDF of the signed request letter) is entered/uploaded into AIS by the EPA lead staff in the program office that will be issuing the EPA determination letter. Once the EPA determination letter is issued, the lead staff will submit to Headquarters via AIS for publication to the ADI public database and a Federal Register Notice. All AIS internal users will use the single sign-on (SSO) LAN ID and password to access the system.

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.

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

No. All users would need to manually enter data into the AIS system data fields, including required header fields under Title, Author, Office, Recipient; rule-related information under “Category”, “References” and “Subparts” and add the incoming request in any format and a PDF of the final EPA response letter.

2.4 Discuss how accuracy of the data is ensured.

The system does not provide extensive data validation, but instead relies on the lead staff providing accurate, complete and timely data entry to establish the determination record with the formal incoming request and EPA determination letter signed by an EPA authorized EPA Official.

2.5 <u>Privacy Impact Analysis</u>: 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 a low risk of unauthorized access to PII. Within AIS, internal interface, only minimal PII is stored. Names of requestors are accessible to EPA staff and managers addressing the formal determination requests, which is contained in the AIS records. Names, email addresses, and office phone numbers of EPA staff assigned to their requests are accessible to EPA staff and managers addressing the formal determination requests, but these data are already available in the EPA Staff Directory on the EPA website.

Names, EPA office affiliation, and EPA email address and EPA LAN ID are available to administrative users only in the system administration menu. This table is used for linking to the WAM for authenticating approved users only.

Mitigation:

Access to the AIS system is limited to authorized internal users (i.e., EPA staff) only and there are privacy controls in place that do not allow external users to access AIS. Each time an internal user logs in, they will be presented with the Terms and Conditions of Use. These terms and conditions should be read before continuing to the next page. Users will need to use their EPA authorized LAN ID and password to access AIS. While the functionality to export certain AIS data elements from the system can occur via the ADI public database, 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 that was provided in the formal incoming request letter.

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 internal users to access AIS. Internal 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. No external users have access AIS.

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 AD/AIS 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.

The data will be read-only unless the internal user is the owner of the determination record and has not yet released the determination to Headquarters for Federal Register notice publication or is an administrator type user.

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.

3.3 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?

Internal users include: US EPA staff in OECA, OAQPS, and EPA Regions 1 through 10.

Contractors to USEPA staff in charge of system administration; the ERG contract supporting the ADI system includes the appropriate FAR clauses).

No external users have access to AIS.

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. AIS is the master data determination record system to allow for publication of the final determination letter and key supporting field data (i.e., rule information, assigned record title and an abstract) to the ADI public database. Since AIS 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:

The ADI/AIS system is a historical data system, so records are retained indefinitely. The privacy risk associated with degeneration of data, deletion or lost of data or huge data storage overtime is low.

Mitigation:

ADI/AIS retention schedules are applied and serves as a taxonomy of information that determines what kind of data assets the system stores, where users are creating intellectual property and how long to keep the data.

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.

Yes. Once applicability determinations are finalized, and the determinations are approved for public consumption, certain data elements stored in AIS, the internal interface, are shared with outside parties through the ADI public website (epa.gov/adi). These data include the final EPA determination letter (.pdf file format), which would show the recipient name and physical address that the letter was sent to, and the EPA staff name that signs the letter as well as the EPA staff name and phone number that is the point of contact for any follow-up questions to provide compliance assistance. The data is used by regulated entities and co-regulators to identify similar questions related to applicability or regulatory interpretation that have come up as part of CAA rule implementation. Only AIS administrator users can authorize the export of data from AIS to ADI.

In addition to the sharing that exists with the ADI website, the lead EPA program office receiving a request may share information stored in AIS, typically by email or during calls, related to the request outside of EPA with co-regulators (delegated states, locals and tribes), at their discretion and following internal guidance to provide a determination response to a requestor.

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

The external sharing of specific AIS data through the ADI public database for access by the public provides compliance assistance to the regulated community and co-regulators to ensure implementing a consistent Clean Air Act compliance program. The general provisions of 40 CFR Parts 60 and 61 allow a source owner or operator to request a determination of whether a rule applies to them or seek permission to use monitoring or recordkeeping which is different from the promulgated standards. These requests have been tracked by the EPA since the 1970s and made public on the ADI website. The AIS data system does not change these general provisions, but instead it just provides a more automatic way to store and disseminate the data to the ADI website. Prior to AIS the data were stored in hard copy or email records in multiple EPA offices.

The AIS data elements not shared with outside parties are intended to keep an internal record of the request and track the EPA response and publication process, which includes the incoming request and status fields (e.g., "Status" category and internal "Comment").

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?

There are no formal agreements for data sharing. Prior to making the data available on the ADI website, the EPA Office of Compliance conducts a thorough QA/QC on the contents of each AIS record that will be shared. As part of this QA/QC, EPA prepares a Federal Register notice based on the contents of AIS and that notice goes through an approval process that consults with all 10 EPA Regions and ultimately final signoff by management, and when needed input from EPA Office of General Counsel. Once the notice is approved, the contents of the notice are uploaded into AIS and then the status is changed within the data system. Only the records with a status of "Request Published on ADI" will be displayed on the ADI public interface. Only AIS Administrator users are authorized to change the status of a record to allow it to be published on the ADI.

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:

There is a low risk of data exposure due to draft determinations being shared outside of the agency with co-regulators (e.g., delegated states). System only allows the records with a status of "Request Published on ADI" to be displayed on the ADI public website.

Mitigation:

EPA will mitigate release of draft determinations outside the agency through internal EPA agency review procedures and AIS system user access restrictions, which prevent the release of draft determinations to the ADI database. The risk associated with sharing privacy-related information in final determination is also low because EPA only shares a minimum number of AIS data fields with outside parties through the ADI public database. The information contained in the final EPA determination letter is the basic facility contact name and facility address. EPA does not publish the letter containing the initial inquiry which may have other contact information (email, phone number) of the requestor. Facility contact name and facility address are considered to be basic data fields necessary to identify and track facilities compliance with CAA regulations.

The submittal of requests for applicability determinations is voluntary and the submitters understand that any final determination responses issued by EPA will become publicly available on the ADI website. Only limited data stored in AIS are made available on the ADI website, after the list of final determinations are approved for publication by EPA management. Only AIS administrator users have the authority to change the status of a determination such that it is published on the ADI website. This data is also available in other EPA data systems and is not providing any extra privacy data to the public.

Internal AIS users are required to follow internal guidance on the process and take training on the system to ensure consistent implementation of the determination response process and proper handling of the determination data in the system.

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?

System only allows us to share a number of AIS internal data fields that is part of the ADI public interface template.

Only the AIS system administrator type users are authorized to publish a determination to

ADI. EPA only shares a minimum number of AIS data fields with outside parties through the ADI public database.

Every AIS user must acknowledge that they are accessing an EPA data system, when logging into AIS and use it according to internal guidance. This acknowledgement includes that their access to AIS is provided for official U.S. Government purposes only.

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 <u>Privacy Impact Analysis</u>: Related to Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

<u>Privacy Risk</u>:

ADI/AIS risk associated with technical safeguards and security measures is low since the AIS user assigned to develop a response or that initiated the AIS record are may edit a record incorrectly.

<u>Mitigation</u>:

User agreements for accessing EPA data systems are required before accessing the AIS system. AIS measures are in place for user type and access to determination records data (e.g., type of data is read-only vs. read-write access). In addition, internal users are required to follow internal guidance on the response process and take training on the system, which includes the 1999 guidance manual on “How to Review and Issue CAA Applicability Determinations and Alternative Monitoring” and any recent standard operating procedures that supplemental this guidance.

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 AIS is a central electronic record data system of Agency determinations and relevant supporting information (e.g., regulatory data). The internal AIS user leading the response to a request will establish the determination record with the incoming request. AIS users that are not the owner of a determination record with read-only access can search records to obtain data to ensure more consistent determination responses to similar requests. AIS determination records' fields also facilitates updating the ADI public database, which contains the final EPA determinations and relevant supporting data.

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. <u>any identifier unique to an individual</u>. Or any identifier that can be linked or is linkable to an individual.)

The request ID (control number which is associated with a record but not an individual) is the master number to track each determination request. When an internal user creates an AIS record with the incoming request this ID is assigned automatically by the data system. The internal users can also search for records by this ID, but only the record owner can make changes to the record. Other regular users with read-only access to AIS can search records to obtain data that can provide assistance to develop a similar response to ensure consistent implementation of the program.

Summary table reports only display control number, title, category of request, the lead office, letter date, and the status category of the request.

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.

Privacy Risk:

The ADI/AIS risk related to ensuring proper use of information is low. The risk is that a AIS user that is the owner of a determination record may edit a record incorrectly.

Mitigation:

Internal user agreement for accessing EPA data systems are required before accessing the system. AIS system controls for accessing type of data are in place, which consist of read-only access for regular users and read-write access for owners of records. In addition, users are required to take training and follow current guidance on the system and response process, which includes the 1999 guidance manual on "How to Review and Issue CAA Applicability Determinations and Alternative Monitoring" and any recent standard operating procedures that supplemental this guidance.

*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: