

PRIVACY IMPACT ASSESSMENT

(Rev. 07/2018)

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 QUALITY SYSTEM

Preparer: ROBERT COATS

Office: 919-541-5448

Date: APRIL 22, 2019

Phone: 919-541-5448

Reason for Submittal: New PIA 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:

AQS collects ambient air pollution data collected primarily by state, local, and tribal air pollution control agencies from thousands of monitoring stations located across the country. AQS also contains meteorological data, descriptive information about each monitoring site is a matter of public record (as mandated by Federal Open Data Policy and laws.)

Note:

These are not the locations of individual persons or organizations, but are only the locations of ambient air monitoring equipment, and quality assurance/quality control information. The Office of Air and Radiation, along with its regional and state partners, rely upon AQS data to assess air quality, assist in attainment/non-attainment designations, develop and evaluate State Implementation Plans for non-attainment areas, perform modeling for permit review analysis, and carry out other air quality management functions.

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?

Federal Register Citation: 40 CFR Part 58

42 U.S.C. 7403, 7405, 7410, 7414, 7601, 7611, 7614, and 7619.

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 – December 19, 2019 but are in process of renewing ATO this month with CIO signature by June.

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.

The information is not covered by the PRA.

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).

The system collects, uses, and maintains the following data elements pertaining to individuals:

- First and last name
- Government agency (State, Local, Tribal, or Federal) that is requesting and authorizing AQS access for the user.
- Address of the agency that is authorizing access for the user.
- Phone numbers of the authorizing agency that can be used to route system notices (e.g. planned outages) to the registered user.
- Email address at the authorizing agency that can be used to route system notices to the registered user.
-

The application does not disseminate any of these data fields.

Note: There is no information about individuals linked to the above name and contact information in AQS. Therefore, by the definitions in NIST 800.53 Appendix J, AQS does not have PII risk.

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

The information is provided by the system users at the time of registration. The user can update the data when they deem necessary.

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.

There are no data validations performed on these fields. This information is used within the application to provide informational messages about activity within the application.

AQS does not provide the information to state, local, and tribal entities; they provide it to AQS. As noted above, the metadata about users is entered when a new user is registered to AQS. This registration requires verification and approval by the designated contact for the State, Local, or Tribal agency requesting that the user be created.

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:

None.

Mitigation:

N/A

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 – AC-2(c): Establishes conditions for group and role membership.

All users may access information pertaining to their own account. Only defined system Account Managers may access account information for other users.

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

Users names and organizational contact information is only stored in a single table (AIRS_USER_PROFILES) in the AQS database. This table is configured under database security so that users can only access the table via the AQS application, and not via ad-hoc tools. The AQS application is configured as follows:

- Normal (non privileged) users: Can only access their own user profile record.
- Privileged users (the AQS Federal user account manager): Can access all user profile records in order to perform account maintenance.

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?

EPA Federal staff identified as “Account Managers” have access to this information.

AQS does not presently have contractor support. If and when a new support contract is put in place, it will the required clauses.

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.

For reasons of data integrity, every change to Ambient Air Quality measurement data is tracked to the user who made the change. Therefore, the name and organizational contact information for users is stored permanently.

There is no EPA Records Control Schedule presently in place. We will create a POA&M in Xacta to create one.

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.
There is no EPA Records Control Schedule presently in Place.

Privacy Risk:

There is a risk that record will be maintained longer than necessary.

Mitigation:

A record control schedule will be developed for this application and/or records.

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. User information is not shared outside of EPA, or with other organizations within EPA

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:

None

Mitigation:

None required. Information is not shared outside of EPA.

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?

Through the implementation of control AC-2(c): Establishes conditions for group and role membership;

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

Since the only personnel who have access to user metadata are Federal AQS staff, their training consists of the annual EPA security and privacy awareness training, and role-based training for system managers.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

None.

Mitigation:

No mitigation strategies currently in place.

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 system keeps the information only so that we can contact users for the following purposes:

- 1) Send a message to users about a bug or other problem with the system, or when there is a significant change in system operations
- 2) To contact an individual user who may be having problems with a system function
- 3) To keep track of the administrative contacts for state and local air agencies.

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

None. A SORN s not required.

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:

None.

Mitigation:

None.

*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:

