United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – 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 Roster.docx

System Name: Drinking Water State-Federal-Tribal Information Exchange System (DW-SFTIES)		**System Owner: Tina Chen**	
Preparer: Tina Chen		**Office: OW**	
Date: 3/10/2026		**Phone: 202-566-0248**	
Reason for Submittal: New PIA			
New: X	Revised: ☐	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s): Development and Implementation			
Definition: ☐	Development/Acquisition: X	Implementation: X	
Operation & Maintenance: ☐	Rescindment/Decommission: ☐		

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 Drinking Water State-Federal-Tribal Information Exchange System (DW-SFTIES) will replace the current Safe Drinking Water Information System (SDWIS) suite of software. The SDWIS suite of software is developed by the EPA and used by primacy agencies (EPA regions, states, territories, tribe) to run their Public Water Supply Supervision (PWSS) program, per the Safe Drinking Water Act (SDWA). The current suite of applications is used by primacy agencies to meet drinking water program data management needs, for example, managing water systems, facilities, legal entities, analysing water sample data to make compliance determinations, violations, enforcement actions, etc.

DW-SFTIES will collect data on water systems and drinking water contamination levels as required by

the Safe Drinking Water Act and support regulations establishing Maximum Contaminant Levels (MCLs), treatment techniques, and monitoring and reporting requirements to ensure drinking water is safe for human consumption.

Section 1. 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?

https://www.epa.gov/dwreginfo/primacy-enforcement-responsibility-public-water-systems

The Safe Drinking Water Act (SDWA) requires EPA to establish and enforce standards that public drinking water systems must follow, including:

- Maximum contaminant levels or treatment techniques
- Monitoring and reporting requirements

EPA delegates primary enforcement responsibility (also called primacy) for public water systems to states and Indian Tribes if they meet certain requirements.

Applicable law, regulations, and guidance:

- Safe Drinking Water Act, 1974, as amended in 1986 and 1996
- Primacy Regulations 40 CFR Part 142, Subpart B, 1976, as amended in 1986
- State Programs Priority Guidance (1992)
- Revisions to Primacy Requirements (1998), 63 FR 23362 codified at 40 CFR Part 142

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 not been completed. We expect the system will be issued an Authorization to Operate in the September/October 2026 timeframe. A third-party assessment has been scheduled for May 25, 2026.

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.

Data from Reginfo.gov

AGENCY: EPA-OW **OMB CONTROL NUMBER:** 2040-0090
EXPIRATION DATE: 06/30/2027 **ICR REFERENCE NUMBER:** 202303-2040-003
TITLE: Public Water System Supervision Program (Renewal)
TOTAL ANNUAL RESPONSES: 1,030,378 **TOTAL ANNUAL BURDEN HOURS:** 3,421,278 **TOTAL ANNUAL BURDEN DOLLARS:** 37,756,000
ASSOCIATED INFORMATION COLLECTIONS:

TITLE	RESPONSES	TIME (HOURS)	COST (DOLLARS)	FORM NAME	FORM NUMBER
Public Water Systems (PWSs)	295,829	1,840,665	36,715,000		
PWSS Program - Laboratories	1,902	42,892	1,041,000		
PWSS Program - Primacy Agencies	732,647	1,537,721	0		

AGENCY: EPA-OW

OMB CONTROL NUMBER: 2040-0090

ICR REFERENCE NUMBER: 202303-2040-003

EXPIRATION DATE: 06/30/2027

TITLE: Public Water System Supervision Program (Renewal)

- EPA ICR No. 0270.47 - Public Water System Supervision Program
- EPA-HQ-OW-2011-0443 (Extension of PWSS Program ICR in March 2023)

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?

Yes, the data will be maintained and stored in the Cloud. EPA's AWS Enterprise Cloud Hosting System.

Section 2. 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).

DW-SFTIES is designed to be used by EPA and State/Territorial/Tribal partners. DW-SFTIES will use agency approved shared service for identity management.

- Enterprise Identity Access Management (EIAM) to authenticate organizational users
- Central Data Exchange (CDX) to authenticate non-organizational users

For the purposes of user account management, the identity management services above may contain the following data elements: the user's name, login ID, work email address, and Organization (EPA or state/territory/tribal organization). This information helps us determine the appropriate user access roles and permissions to the system data and data services.
The DW-SFTIES system will be able to collect and maintain these data elements:

- Title
- First Name
- Middle Initial

- Last Name
- Suffix
- Professional Title
- Alias Name
- Job Title
- (Business) Phone Numbers
- (Business) Email addresses
- (Business) Website Info
- Physical (Business) address (street, city, state, country, zip)

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

Sources of information:

- Primacy agency staff (EPA regions, states, territories, tribe)
- Water system owners and employees
- Lab owners and employees
- EPA HQ staff/programs
- Directly from the user
- Migrated from legacy system

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

State agencies and EPA may rely on external data sets managed by State agencies to validate information, such as professional qualifications and operator license/class data on water system operators. These data sets are usually publicly available information collected/maintain by state agencies.

The system does not include any direct connections/integrations with external data systems and/or commercial sources of data.

2.4 Discuss how accuracy of the data is ensured.

Accuracy of PII is ensured through the following methods:

- Manual data review by primacy agency staff
- Automated or manual data quality check reports
- Data collected and/or verified during phone calls, emails, site visits, inspections with regulated entities
- Routine data requests sent to regulated entities to validate information either by email or postal mail
- Data validation checks built into the application user interface, for example, duplication checks, data format checks, data length, area code validation, zip code validations, etc.

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:

The system will collect and store the names of legal entities; individuals associated with regulated water systems. While this information may be publicly available through generic search engines (i.e. Google, Bing, etc.), it could potentially be used to tie an individual to a specific employer and/or state.

Mitigation:

We plan to implement all applicable NIST 800-53 Rev.5 Security and Privacy controls to ensure protection commensurate with the system categorization. This system will limit data access to authorized individuals on a need to know/access basis, and controls individuals' ability to access and alter records with the system. More details can be provided when more aspects of the system and system components are developed.

Section 3. 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 system has implemented access controls to prevent unauthorized access to data.

- Database design/organization isolates one primacy agency's data from another via explicit schema access controls.
- Usage of the Agency's multifactor authentication compliant identity management service, EPA's Central Data Exchange

Implementation of additional application-level role-based access controls will further restrict data access (read/write) for each module/data area within each database schema. Users will need to be explicitly granted permission to access data (read/write).

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

- Access controls identified in 3.1 will be documented in system documentation and relevant user guides.
- Inherited access controls from EPA's CDX and/or Enterprise Identity Access Management services will be documented in Xacta.

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 HQ staff -- EPA Admins and system users
- Primacy agencies (EPA regions, states, territories, tribe) – System users
- Support contractors for EPA HQ and primacy agencies – Yes, the appropriate FAR clauses are included in the contract.

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.

Data collected and maintained in this system will be subject to both federal and state record retention requirements, some data elements may have an explicit timeframe, while other data elements may require permanent retention.

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:

N/A.

Mitigation:

N/A.

Section 4. 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 governments, 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, the information with be shared and accessed by primacy agencies (EPA regions, states, territories, tribes). Data will be accessed based on an individual's account permissions per system/application-level access controls.

- Information may also be shared, as needed, with DHS, FEMA, and other relevant federal/state agencies in the event of an emergency response/disaster declaration by states, territories, and tribes.

- Data may also be shared with other relevant federal/state agencies, as needed, per valid MOUs.

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

The Safe Drinking Water Act (SDWA) requires EPA to establish and enforce standards that public drinking water systems must follow, including:

- Maximum contaminant levels or treatment techniques
- Monitoring and reporting requirements

EPA delegates primary enforcement responsibility (also called primacy) for public water systems to states and Indian Tribes if they meet certain requirements.

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?

Individuals with System Administration access will review and approve access to the system by organizations within EPA and outside. EPA program managers will coordinate with other Federal Agencies, as needed, if access is requested per applicable MOUs.

4.4 Does the agreement place limitations on re-dissemination?

N/A. No existing information agreements are in place.

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:

Individuals or organizations outside the agency may gain access to system data based on legitimate use/business need.

Mitigation:

Access will be granted to users with a specified and approved use-case/business need. We plan to implement all applicable NIST 800-53 Rev. 5 Security and Privacy controls to ensure protection commensurate with the system categorization.

Section 5. 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?

DW-SFTIES included both system and application-level access controls to limit data access by users of the system.

The data from this system is not meant for direct public dissemination and sharing by the EPA, and therefore, public access will not be allowed.

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

- All EPA employees are required to take Annual Information Security and Privacy Awareness Training, which includes privacy elements.
- EPA contractors also have annual security training requirements based on their data access.
- System users will be provided with training and user guide documentation.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

If system auditing and accountability measures are not implemented, data could potentially be at risk of alteration and/or repudiation.

Mitigation:
The DW-SFTIES system design includes that all users of the system will be given a unique user identification (ID) with personal identifiers, and all interactions between the system and the authorized individual users are logged. Activity logs ensure any alterations are properly and sufficiently accounted for. Audit logs are protected against unauthorized access.

We plan to implement all applicable NIST 800-53 Rev. 5 Security and Privacy controls to ensure protection commensurate with the system categorization.

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.
DW-SFTIES is a legacy modernization project to replace the current Safe Drinking Water Information System (SDWIS) suite of software. The SDWIS suite of software is developed by the EPA and used by

primacy agencies (EPA regions, states, territories, tribe) to run their Public Water Supply Supervision (PWSS) program, per the Safe Drinking Water Act (SDWA).

The current suite of applications is used by primacy agencies to meet drinking water program data management needs, for example, managing water systems, facilities, legal entities, analysing water sample data to make compliance determinations, violations, enforcement actions, etc.

DW-SFTIES will collect and manage data on water systems and drinking water samples data as required by the Safe Drinking Water Act and supporting regulations establishing Maximum Contaminant Levels (MCLs), treatment techniques, and monitoring and reporting requirements to ensure drinking water is safe for human consumption.

The DW-SFTIES system will need to collect and maintain the data elements below for the purposes of user management and data management of co-regulators and regulated entities.

- Title
- First Name
- Middle Initial
- Last Name
- Suffix
- Professional Title
- Alias Name
- Job Title
- (Business) Phone Numbers
- (Business) Email addresses
- (Business) Website Info
- Physical (Business) address (street, city, state, country, zip)

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: X No ☐ 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 system is designed to allow data retrieval by users based on the permissions associated with their user account. Primary types of access include read-only access, write-access, and no-access.

There are very limited use-cases for data to be retrieved by a personal identifier. In those limited scenarios, the following identifiers can be used: unique user ID, First Name, and/or Last Name. The system **does not** collect nor manage any sensitive PII data.

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?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

DW-SFTIES collects and manages data on individuals as it relates to their professional/business capacity and association with EPA, a primacy agency, and/or regulated entities (labs and water systems). The majority of this information is publicly available through generic search engines (i.e. Google), and/or shared publicly by individual primacy agencies (state, tribal, territorial agencies) and organizations.

The collection of names and contact information for legal entities is required for accurate data management by EPA and primacy agencies.

Only approved and registered users can access the data within the DW-SFTIES.

All applicable NIST800-53 Rev. 5 Security and Privacy controls will be implemented to ensure protection commensurate with the system categorization.

Controls in place at each level:

- Authentication provider controls: multi-factor identification, identity proofing
- Database controls: (only accessible via services with the appropriate permissions, dedicated schema for each primacy agency with access controls)
- Application controls: permissions/roles limit access to the people who need access as related to their official duties

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:

The system collects and stores the names and organizational contact information of legal entities. While this information may be publicly available through generic search engines (i.e. Google), and/or shared publicly by individual primacy agencies (state, tribal, territorial agencies) and organizations, it could be used to tie an individual to a specific employer.

Mitigation:

All applicable NIST800-53 Rev. 5 Security and Privacy controls will be implemented to ensure protection commensurate with the system categorization.

System components and data will be hosted in an EPA managed cloud environment. Multiple levels of security are maintained with the computer system control program. This system limits data access to authorized individuals on a need to know/access basis and controls an individuals'

ability to access and alter records within the system. All users of the system will be given a unique user identification (ID)with personal identifiers, and all interactions between the system and the authorized individual users are logged.

Controls in place at each level:

- Authentication provider controls: multifactor identification, identity proofing
- Database controls: (only accessible via services with the appropriate permissions, dedicated schema for each primacy agency with access controls)
- Application controls: permissions/roles limit access to the people who need access as related to their official duties

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

EPA's Central Data Exchange Privacy Statement is presented to the user when registering for a CDX account.

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?

An individual can choose not to register/create a CDX account. A warning notice and privacy statement is presented to the user before account creation. Terms and conditions are presented to the user to review and accept. A user must take action to accept the terms and conditions before proceeding with account creation. Users can terminate their accounts at any time.

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:

Risks associated with potentially insufficient notice and opportunity to decline or consent.

Mitigation:
The CDX Terms and Conditions correspond to the purpose of the project and stated uses by explaining to the user how their information will be used for official US Government purposes only and for use by a US Government information system.

This is consistent with the uses of information by DW-SFTIES since DW-SFTIES is an official US Government information system.

Users must actively accept the terms and conditions before proceeding with account creation.
The user can terminate their account at any time.

Section 8. 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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted.

Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

For more information, individuals can access EPA's public website on "EPA's Implementation of the Privacy Act" (https://www.epa.gov/privacy) where they can submit a Privacy Act request.

Users of the system are able to access their own profile information and records they are associated with.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

For more information, individuals can access EPA's public website on "EPA's Implementation of the Privacy Act" (https://www.epa.gov/privacy) where they can submit a Privacy Act request.

Users of the system are able to access their own profile information and records they are associated with. The user may have required permissions to correct data about themselves. Users of the

system can also contact their system administrator for their applicable primacy agency and/or organization to correct inaccurate or erroneous information on their behalf.

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 Freedom of Information Act (FOIA).

Privacy Risk:

The system may contain inaccurate or erroneous information for an individual.

Mitigation:
Users of the system are able to access their own profile information and records they are associated with. The user may have required permissions to correct data about themselves.

Users of the system can also contact their system administrator for their applicable primacy agency and/or organization to correct inaccurate or erroneous information on their behalf.

I attest as the Agency Privacy Officer that the **Drinking Water State-Federal-Tribal Information Exchange System (DW-SFTIES)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY
Digitally signed by ROBERT KELLY
Date: 2026.05.08 10:16:00 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA