EPA United States
Environmental Protection
Agency

PRIVACY IMPACT ASSESSMENT

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

System Name: Publicly Owned Treatment Works Screener Questionnaire Registration Application	
Preparer: Brian D'Amico	**Office:** Office of Water
Date: 4/23/2018	**Phone:** 202-566-1069

Reason for Submittal: New PIA X__ **Revised PIA**____   **Annual Review**_____

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:

This system will house contact information for respondents of a technical survey. The technical survey is designed to ascertain the treatment capability of publicly owned sewage treatment plants (POTWs). This very limited PII we are requesting is contact info for a facility representative in the event we have a question about the technical responses they submit. We are not asking for home addresses, personal phone numbers, or any other private information. All of the information we collect as part of this survey, including the PII contained within this system, would be subject to a FOIA request, as POTWs are unable to claim CBI for their treatment works. The limited contact info we are requesting would be the same information available on their respective websites.

Section 1.0 Authorities and Other Requirements

    1.1   **What specific legal authorities and/or agreements permit and define the collection of information by the system in question?**

This is a voluntary survey.

1.2 Has a system security plan been completed for the information system(s) supporting the system?

Yes, a system security plan has been completed for the Business Automation Platform (BAP). Timothy Hinds is the POC for additional details.

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.

A record control schedule has not been issued. The second FRN (December 29, 2017) requests the OMB control number for the collection. An OMB control number for the corresponding ICR for this information collection has not yet been issued.

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, job title, business phone number, and business email address will be collected from staff at publicly owned treatment works (POTWs) to facilitate registration for a survey. POTW facility contact information will be entered and maintained.

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

The application will reside within EPA's Business Automation Platform (BAP), a Salesforce instance on Salesforce's Government Cloud. The application will house facility name, NPDES ID, and address information about POTW facilities gathered from EPA's Permit Compliance System (PCS), Integrated Compliance Information System (ICIS), and Facility Registry Service (FRS). In addition, the application will collect contact information—name, job title, business phone number, and business email address—from facility representatives when they request a link to a questionnaire about their facility.

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

The system is populated with facility name, location, and National Pollutant Discharge Elimination System (NPDES) ID from publicly available data sources (e.g., EPA ICIS-NPDES, FRS, and state public records) allowing respondents to identify their facility and

obtain the questionnaire.

2.4   Discuss how accuracy of the data is ensured.

N/A

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.

<u>Privacy Risk</u>:

Given that all of the data in the system is already publicly available and the purpose is simply to track the distribution of a voluntary survey, the risks associated with technical failures, malevolent third parties, and/or human error are not significant.

<u>Mitigation</u>:

None needed.

Section 3.0 Uses of the Information

The following questions require a clear description of the system's use of information.

3.1   Describe how and why the system uses the information.

The primary purpose of the application is to allow POTW facilities to register for a voluntary questionnaire and to ensure that multiple questionnaires are not completed for a given facility. The PII—name, job title, business phone, and business email—is collected for a variety of reasons: (1) The email address is used to send the electronic survey link, (2) the name and phone number allows EPA to follow up with individuals who request a link but never complete the survey, and (3) the job title and first and last initial are displayed to any user who attempts to request an already-requested survey link.

3.2   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.)*

If a potential registrant attempts to request an already-requested survey link, s/he will be shown the job title and first and last initials of the person who originally requested the survey link, thereby facilitating internal follow up by the registrant. Each facility is assigned a unique survey ID. Users who register can look up their facility in the system by facility name, NPDES ID, or city/state.

3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?

NA. (The system does not retrieve information by personal identifier.)

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

A SORN entry is not required for this tool, per ISO: Marshall Mansfield, 3/27/2018.

3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.

No. The system only allows potential registrants to locate their POTW facility via NPDES ID or facility address in order to request a link to a voluntary survey about that facility.

3.6 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:

N/A

Section 4.0 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.

4.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

No notification is provided; however, the header text in the application states that information provided by the user will only be used to facilitate the distribution of the POTW questionnaire. The user only enters the system after receipt of a letter from EPA, the state, or a trade association. The letter indicates the system is for registration for the technical survey.

4.2 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?

The fields—name, job title, business phone, and business email—are all required if the requestor wishes to receive a link to the survey; however, the application indicates that the questionnaire itself is voluntary. As indicated above, the user only enters the system after receipt of a letter from EPA, the state, or a trade association.

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

<u>Privacy Risk</u>:

None

<u>Mitigation</u>:

N/A

Section 5.0 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.

5.1 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?

Users of the web form will have read-only access to POTW facility names and addresses. (This is already publicly available information.) As for PII, web form users will only be able to submit information; they will not have access to the information provided by other users. The exception to this is that if a user attempts to request an already-requested survey, the application will display the job title and first and last initials of the person who requested it.

Within Salesforce, access to information is controlled by user accounts and profiles, so only individuals who have specifically been given access to the system will be able to see the submitted PII. EPA's contractor is the only non-EPA user with access to the system, and will have user/viewer only access.

5.2 Are there other components with assigned roles and responsibilities within the system?
None.

5.3 Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition

Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

EPA and contractors for this work. Contractors will not have administrative privileges but will be able to view records. Contract states "All work performed under this contract shall adhere to the clause EPAAR 1552.211-79, "Compliance with EPA Policies for Information Resources Management", which requires adherence to all Agency directives for performance of any IRM related work." The contract includes a table of Federal Policies and Regulations that must be observed, including the Privacy Act of 1974, 5 U.S.C Section 552a. .

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

Within Salesforce, access to information is controlled by user accounts and profiles, so only individuals who have specifically been given access to the system will be able to see the submitted PII.

5.5 Explain how long and for what reason the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Data will be used for a short time period (~3 months) to allow facilities to complete a questionnaire. The survey questionnaire is a one-time collection. No, a record control schedule has not been issued. Upon completion of the survey, including follow-up activities and quality assurance reviews, the Salesforce application will not be retained.

5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No.

5.7 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 with the stated purpose and mission of the system.

Privacy Risk:

None

Mitigation:

N/A

Section 6.0 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.

6.1   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 information is shared outside of EPA and their contractor for this work.

6.2   Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

N/A

6.3   Does the agreement place limitations on re-dissemination?

No.

6.4   Describe how the system maintains a record of any disclosures outside of the Agency.

N/A

6.5   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

6.6   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:

N/A

Section 7.0 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.

7.1 What are the procedures that allow individuals to access their information?

There are no procedures in place. The only information collected about individuals—name, job title, business phone, and business email—would have been provided by those individuals themselves.

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

None.

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

N/A

7.4 <u>Privacy Impact Analysis</u>: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

<u>Privacy Risk</u>:

None

<u>Mitigation</u>:

N/A

Section 8.0 Auditing and Accountability

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

8.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

User accounts and profiles will ensure that only individuals who have specifically been given access to the system will be able to see and use the submitted PII.

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

The users of the front-end web form will not have access to any PII, except whatever they themselves have entered. All users with back-end access to Salesforce have already signed confidentiality agreements and have undergone training in the proper use of PII In addition, all users (both EPA and contractors) will have completed the 2018 Information Security and Privacy Awareness Training (IPSAT) and the 2018 Records Management Training, in accordance with EPA policy.

8.3   Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

None

Mitigation:

N/A