

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)

(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%20Roster.docx

System Name: Research on Customer Participation in Lead Service Line Replacement Programs	System Owner: Heather Klemick
Preparer: Heather Klemick	Office: AO/OP/NCEE/RPSD
Date: 9/30/20	Phone: 202-566-2522
Reason for Submittal: New PIA <input checked="" type="checkbox"/> Revised PIA <input type="checkbox"/> Annual Review <input type="checkbox"/> Rescindment <input type="checkbox"/>	
This system is in the following life cycle stage(s):	
Definition <input checked="" type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f)</u>.	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45)</u>.	

Provide a general description/overview and purpose of the system:

We are planning to obtain existing administrative data from Trenton Water Works on the properties in their service area for a research project on customer participation in their Lead Service Line Replacement program, as well as existing administrative records from Isles, Inc. about properties in the Trenton area that have been inspected for lead hazards. We will use the property address field to merge these two data sources and to merge in publicly available data on neighborhood characteristics from Census and property characteristics from the property tax assessment database for Mercer County, New Jersey. The data that we receive will be in an Excel spreadsheet, we will then conduct a statistical analysis of the data and write up the results for publication.

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?

Executive Order 13707, “Using Behavioral Insights to Better Serve the American People,” encourages federal agencies to use behavioral science insights when designing policies and programs. This data collected will allow the researchers to study how behavioral insights can be applied to improve cost-effective implementation of Lead Service Line Replacement programs.

By using data to assess the effectiveness of Lead Service Line Replacement programs, this project also falls under the scope of the Foundations for Evidence-Based Policymaking Act of 2018 and OMB Circular A-11. OMB Circular A-11, “Preparation, Submission, and Execution of the Budget,” states that, “Agencies should strengthen the use of evidence (defined in section 200.22) and data to drive better decisionmaking and more effectively deliver on mission.” Section 200.22 explains, “As defined by 5 U.S.C. 311(3), ‘evaluation’ means an assessment using systematic data collection and analysis of one or more programs, policies, and organizations intended to assess their effectiveness and efficiency. Evaluations can provide critical information to inform decisions about current and future programming, policies, and organizational operations.” Finally, Circular A-11 notes that, “The Foundations for Evidence-Based Policymaking Act of 2018 (or “Evidence Act”) advances data and evidence-building functions in the Federal government by statutorily mandating Federal evidence-building activities, open government data, and confidential information protection and statistical efficiency.”

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?

This is not an actual system or application but a process that involves the EPA receiving Excel documents from Trenton Water Works. The data captured in the Excel spreadsheets will be saved to a shared folder on OneDrive with access granted to each of the team members working with this data. The agency’s O365 OneDrive is a secured Moderate-Environment system that retains EPA employee stored/shared data. The ATO and associated security documentation is a part of the agency’s Enterprise Services System (ESS), General Support System which falls under the control of the Office of Mission Support (OMS). This ATO is dated to expire on December 11, 2020.

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.

An Information Collection Request (ICR) is not 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?

Yes, the data will be stored on the MSO365 One Drive - SaaS.

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 data consist of existing administrative records compiled by Trenton Water Works (TWW) on properties in their service area with suspected lead service lines. The data include property address; length and diameter of the service line; whether the property was contacted to participate in TWW's Lead Service Line Replacement Program; whether the property owner registered to participate in program; date when replacement was conducted. We will also have the option to obtain data on the volume of water consumption recorded at the water meter for the property. Authorized users will receive the data as an excel spreadsheet by email or from a secure FTP site. Authorized users will not disseminate the data to anyone else.

The data will also include records from Isles, Inc., a community organization in Trenton, NJ, about properties that have been inspected for lead hazards. These data will include the property address; whether a lead hazard inspection occurred; when the inspection occurred; and the measured concentration of lead in the tap water sample.

The TWW and Isles, Inc. data do not include information about individuals living at the properties. The data will be matched on the basis of property address with publicly available Census data on neighborhood characteristics and publicly available property tax assessment records from Mercer County, NJ. Property tax assessment record include property owner name and other property characteristics, such as property type, year constructed, and assessed value.

2.2 What are the sources of the information and how is the information

collected for the system?

Trenton Water Works (TWW) and Isles, Inc. are the sources of the data. TWW collects and maintains data on property information for operational and billing purposes. Isles collects and maintains data for operational purposes.

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

Yes. We will be linking the TWW and Isles administrative records with publicly available data from the Census and publicly available property tax assessment records from the state of New Jersey.

2.4 Discuss how accuracy of the data is ensured.

The institutions that collect the data (Trenton Water Works, Isles Inc., Census, and New Jersey Division of Taxation) are responsible for ensuring accuracy of the data.

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:

There is a small risk that the data on properties' service line material, participation in the Lead Service Line Replacement program, participation in a lead hazard inspection program, or concentration of lead in tap water samples could be released to non-authorized users.

Mitigation:

Only authorized users will have access to the data, and access controls described in 3.1 will be used. In addition, the data are not sensitive (i.e., no SSN, health, or financial information), so the harm caused by this risk is minimal.

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. Data will be stored electronically, and only authorized users will have access. There will be three authorized users total, and all of them will have access to all data elements. All authorized users are EPA employees (not contractors) included on Institutional Review

Board (IRB) applications. Access will be restricted to authorized users by requiring computer log-on with unique user accounts, PIN numbers, and FIP cards. Data will be uploaded to individual users' local hard drives and the MS0365 One Drive, thus preventing access by anyone other than the three authorized users. The controls meet the moderate security controls required by NIST publication 800-53 revision 4, including 2-factor authentication (PIN number and FIP card).

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

The access controls identified in 3.1 will be documented in our IRB application.

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?

Three authorized users (all EPA employees) will have access to all data elements. No contractor will have access.

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.

We estimate that the data will need to be retained for approximately four years to allow for data cleaning and merging, data analysis, write up of research papers, revision of research papers, and publication of research papers. This project will use the existing **EPA Records Schedule 1035 and NARA Disposal Authority DAA-0412-2013-0021-0005** (<http://intranet.epa.gov/records/schedule/final/1035.html>)

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 small risk that property-specific data will be released to non-authorized users will remain during the length of time the records are retained. The schedule is determined by the research needs and the length of time to publish aggregate results in peer-reviewed journals.

Mitigation:

Only authorized users will have access to the data the entire time it is stored in EPA systems. Records will be permanently deleted consistent with NARA Disposal Authority DAA-0412-2013-0021-0005 when no longer needed.

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, EPA will not share individual-level property data received from Trenton Water Works or Isles Inc. with any systems, agencies, governments, or other external parties. The authorized users are collaborating with non-EPA researchers on this project based at the University of Chicago, but we will not share the data with these non-EPA researchers. The University Chicago researchers may share data with EPA authorized users through a secure FTP site, but EPA will not share data with them. Research results, including aggregate statistics (but no individual-level data), will be disseminated in research reports or peer-reviewed journals.

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

Disseminating research results through working papers and peer-reviewed publications is consistent with the purpose of the project, which is to gain insights about cost-effective lead service line replacement programs and share these insights with public water systems and the research community in order to aid in implementation of the Lead and Copper Rule under the Safe Drinking Water Act.

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?

Not applicable because EPA will not share individual data with any systems, Departments/agencies, governments, or other external parties.

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:

None because individual data are not shared outside of the agency.

Mitigation:

None. Only aggregate statistics (no individual data) are disseminated.

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 as stated in Section 6.1?

Review by the Institutional Review Board (IRB) for the initial project will ensure that the information is used as stated in Section 6.1. In addition, the IRB will review annual updates about our project.

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

All authorized users will take annual EPA Information Security and Privacy Awareness Training identifying the user's role and responsibilities for protecting information resources, as well as consequences for not adhering to the policy.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Risk would occur if authorized users are not trained properly on privacy accountability.

Mitigation:

Annual Information Security and Privacy training is required to be completed by all EPA staff. Staff not completing the training are locked out of the network.

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 three authorized users are all research economists at EPA's National Center for Environmental Economics and will use the data for a research study on customer participation in lead service line replacement. This study aims to provide insights relevant to implementation of the Lead and Copper Rule under the Safe Drinking Water Act on cost-effective approaches for public water systems designing customer lead service line replacement programs.

- 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 dataset is designed to conduct large-scale statistical analysis to examine factors affecting customer participation in lead service line replacement programs. It is not designed to retrieve individual records. Users will only retrieve summary statistics (e.g., means) aggregated by geographic areas such as county, zip code, or Census tract.

- 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?**

In order to mitigate against the release of Personally Identifiable Information, we have planned to put in place the controls described in 6.4.

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.

Data will be stored electronically, and only authorized users will have access. There will be three authorized users total, and all of them will have access to all data elements. All authorized users are EPA employees (not contractors). Access will be restricted to authorized users by requiring computer log-on with unique user accounts, PIN numbers, and FIP cards. Data will be uploaded only to individual users' local hard drives and the MS0365 One Drive, thus preventing access by anyone other than the three authorized users. The controls meet the moderate security controls required by NIST publication 800-53 revision 4, including 2-factor authentication (PIN number and FIP card).

Privacy Risk:

There is a small risk that the data on properties' service line material, participation in the Lead Service Line Replacement program, participation in a lead hazard inspection program, or concentration of lead in tap water samples could be released to non-authorized users. However, these data are not sensitive (i.e., no SSN, health, or financial information), so the harm caused by this risk is minimal.

Mitigation:

Only authorized users will have access to the data, and access controls described in 3.1 will be used.

***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 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: