United States Environmental Protection Agency

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: Consent for Access to Property – Soil Gas Safe Communities Study, Database	**System Owner:** Brian Schumacher
Preparer: Brian Schumacher	**Office:** ORD/CEMM/EPD
Date: 1/30/24	**Phone:** 706-355-8001
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:

Vapor Intrusion (VI) is the migration of hazardous vapors (e.g., radon, solvents, and petroleum products) from a subsurface contaminant source into an overlying building or structure via any route, opening, or conduit. The overall purpose of the research project is to examine the protectiveness of the Indicators and Tracers (IT) approach, which uses simple to measure IT (e.g., temperature, pressure, use of meters which provide large numbers of data points) as compared to the "traditional" standard chemical sampling process

(e.g., using advanced laboratory analyses with few data points), to determine when to collect indoor air and/or soil gas samples to estimate the maximum reasonable exposure of the residents to the hazardous vapors.

The approach to be taken is to: (a) develop criteria for the soil gas safe community designation with VI experts and from the literature, (b) prepare quality assurance project plan, (c) select a community willing and interested in being designated a Soil Gas Safe Community, and (d) conduct a pilot study at that community. The pilot study involves placing a radon detector in the residence and periodically collecting indoor air samples by placing a sampler in the residence for a week and collecting it the following week. Over the course of 9+ months, 12 samples will be collected per residence.

Access is needed to allow placement of radon meters and the collection of samples. Access consent forms will be collected and stored by a cleared contractor on EPA-approved ORD file folders under the ORD Enterprise General Support System (GSS).

Onsite information about the occupant/owner's participation will be recorded on paper and given a structure code (e.g., RP-1). Paper documents containing PII will not be left unattended. When documents containing PII are not being used they will be secured in a locked cabinet. When documents containing PII are transferred to digital form, the documents will be shredded with a cross-cut shredder. The contractor will use the EVDI virtual desktop to transfer PII to EPA-approved ORD file folders.

After access is granted and documented, these records containing PII will only be used if the individual residents request the data at the end of the project and they will receive only their data. Only the contractor can retrieve PII, and they will retrieve by the assigned structure code, not by name or other PII. The rest of the project will use the structure code as the only identifier. For research and reporting purposes, structure code will be used with no PII.

Analytical (e.g., radon and hazardous chemical concentrations) and ancillary data (e.g., temperature, pressure, snow fall, etc.) generated or gathered by the contractor and/or EPA will be maintained in a separate database by the contractor and submitted to EPA during and at the conclusion of the project.

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?

Responses to this collection of information are voluntary under the National Contingency Plan (NCP) § 300.415 (a) (n) (3) (i).

Resource Conservation and Recovery Act (RCRA).

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?

Data is stored on ORD file folders under the ORD Enterprise General Support System. The ORD Ent. GSS ATO expires June 30, 2024.

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.

N/A

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?

N/A

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).

Owner Name, Address, Phone Number, Email Address, and Owner Signature.

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

The source of information is an individual visit to a home or residence (e.g., apartment, condominium). If the owner is leasing a home or residence, and does not reside nearby, the source of information is a phone conversation.

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, but all information is publicly available through multiple sources including public tax records.

Discuss how accuracy of the data is ensured.

Information is obtained directly from resident or building owner.

2.4 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 some privacy risk related to accuracy and nature of information. Participation in the study is voluntary and a resident must express interest in participating in the research program prior to gathering information via personal visit(s). Information to be gathered are name, phone number, address, and email (if available). The estimated number of participants in the study is 15.

Mitigation:

Inherited and system specific controls described in NIST 800-53 are deployed on ORD GSS that hosts this sub-system to protect the information.

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?

Per ORD Enterprise GSSs, all the access control levels are inherited from the ORD Ent. GSS: Users authenticate to ORD desktops and servers using Enterprise Identity & Access management credentials. Designated system administrators and researchers/scientists are granted access to their information on a need-to-know basis, Enterprise GSS systems reside on the Intranet and are not publicly available or accessible from the Internet.

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

Per ORD Enterprise GSS PIA, access control policy/procedure documentation is inherited from the ORD Ent. GSS:

ORD Enterprise GSS systems are integrated with Enterprise Identity and Access management. ORD GSS systems are not publicly available or accessible from the Internet. The integration and accessibility information are documented in the associated system security plan.

ORD GSS systems use Enterprise Identity and Access management credentials. Only the individuals selected to participate and/or oversee the study will have access to the applicable study data/information stored on GSS systems.

The AC policy is Directive CIO 2150-P-01.3 that applies to *all EPA systems.* It is published at https://www.epa.gov/system/files/documents/2023-06/information_security_access_control_procedure.pdf

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?

Only the contractor has access to the data/information in the system. FAR 52.224-1 and 5.224-2 are currently not included in the contract. A modification will be added to include these 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.

EPA Records Schedule 1004 will be followed with destruction of records 10 years after completion of the research project.

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 risk is that the records could be retained longer than needed, and the longer they are maintained, the greater the risk of accidental or intentional disclosure.

Mitigation:

The EPA Records Schedules will be strictly followed. Periodic reviews (at least annually) of retention schedule will be conducted to ensure records are retained according to schedule and continuing need Every record will be destroyed at the end of its predetermined retention period as described in Section 3.5.

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.

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:

N/A

Mitigation:

N/A

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?

ORD GSS systems use Enterprise Identity and Access management credentials. Only cleared contractors and EPA research staff who oversee the study will have access to study data. Only the cleared contractor will use the EVDI virtual desktop to transfer initial PII to EPA-approved ORD file folders. After access is granted and documented, these records will only be accessed if the individual residents request the data at the end of the project and they will receive only their data. Only the contractor can retrieve records, and they will retrieve by the assigned structure code, not by name or other PII.

Control of the PII information will follow controls, such as NIST IDs DM, IP, UL, and SE, in Appendix J of the NIST 800-53, rev 4 document.

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

Annual Information Security Awareness and Privacy Training is required for all EPA federal and contractor staff. Additionally, annual training on data protection and privacy, which includes PII in general, is required by the contractor. The RTI training course is called: Privacy at RTI. Depending on the type of project and IRB determination, staff may have to take project-specific trainings or get their CITI certification (certificate available upon request for RTI task lead).

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

The risk of unauthorized disclosure of or changes in data is very low with proposed administrative and security procedures. Control of the PII information will follow controls, such as NIST IDs AR and ULin Appendix J of the NIST 800-53, rev 4 document.

Mitigation:

ORD GSS systems use Enterprise Identity and Access management credentials. Changes can only be made by authenticated users.

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 pilot study involves placing a radon detector in a residence and periodically collecting indoor air samples. Access consent forms are completed to allow placement of radon meters and the collection of samples. Onsite information about the occupant/owner's participation

will be recorded on paper and given a structure code (e.g., RP01). The contractor will use the EVDI virtual desktop to transfer PII to EPA-approved ORD file folders.

Records containing PII will only be used if an individual resident requests the data at the end of the project. They will receive their data only. Only the contractor can retrieve PII. Analytical (e.g., radon and hazardous chemical concentrations) and ancillary data (e.g., temperature, pressure, snow fall, etc.) generated or gathered by the contractor and/or EPA will be maintained in a separate database by the contractor and submitted to EPA during and at the conclusion of the project.

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.)

No, information will be retrieved by structure code (e.g., RP01), not a personal identifier. Only the contractor can retrieve PII, and they will retrieve by the assigned structure code, not by name or other PII. For research and reporting purposes, structure code will be the only identifier.

Data collected will be organized by structure code number (e.g., RP0 1 that is assigned to the address rather the individual) and a non-name identifier such as "adult female" or an initial "JJ." The names of the persons conversed with would not be recorded, but initials or a description as in "adult male tenant" or "adult female property owner" can be included.

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.]

Risk assessment has been performed via the ORD GSS PTA and PIA and this assessment.

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.

<u>Privacy Risk</u>:

The risk of unauthorized access to and mishandling of participant's PII data.

<u>Mitigation</u>:

ORD GSS systems are not publicly available or accessible from the Internet, and use Enterprise Identity and Access management credentials. Access is only given to authenticated users. Only the contractor can retrieve PII, and they will retrieve by the assigned structure code, not by name or other PII. Analytical data and PII data are kept in two separate databases.

*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: