

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: Region 2 LAN	System Owner: Stephanie Montrallos
Preparer: May Wong	Office: US EPA, Region 2, MSD-IRMB
Date: January 1 2024	Phone: 212-637-3327
Reason for Submittal: New PIA _____ Revised PIA _____ Annual Review <u> X </u> Rescindment _____	
This system is in the following life cycle stage(s):	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input checked="" 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 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 USEPA Region 2 LAN is a general support system providing distributed application and telecommunications support for USEPA Region 2 offices located in New York, New Jersey, and Puerto Rico.

Distributed applications residing on the U.S. EPA Region 2 LAN include, but are not limited to:

- Word-processing applications
- Spreadsheet packages, such as Excel
- Geographic Information Systems
- Enterprise database applications, such as ORACLE

The information processed on the USEPA Region 2 LAN includes, but is not limited to:

- General information
- Documents
- Enforcement data
- Monitoring information
- Budget information
- Geographic information
- Personnel information

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?

Region 2 LAN does not collect PII. The system stores PII collected under these federal authorities: Federal Travel Regulation (FPMP 101-7), E.O. 11609 of July 21, 1971, E.O. 11012 of March 27, 1962, E.O. 9397 of November 22, 1943, and 26 U.S.C. 6011(b) and 6109, Telework Enhancement Act of 2010 (December 9, 2010); Public Law 111–292, Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) Section 11(a)(1).

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. June 1, 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.

No ICR 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?

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 use, dissemination and maintenance of the PII data elements is managed by Region 2 personnel for Regional use and support in all aspects of Regional functionality. PII data elements are not collected by the Region 2 LAN but can be stored on servers or desktops.

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

PII data elements are not collected by the Region 2 LAN, The system is used to store the information in electronic data files..

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.

The Region 2 LAN is only used to store the information in electronic files.

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 risks associated with storing information within the Region 2 LAN is individuals store PII on the LAN.

Mitigation:

Implementing the required security and privacy controls in NIST SP 800-53, assessing the system annually and conducting continuous monitoring of the system

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?

The system has different access control levels which are users, desktop and server administrators. These access is granted based on roles and responsibilities.

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

Region 2 access control levels are documented in the account management SOP.

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?

PII information is accessible only to authorized R2 personnel. No contractors access applications with PII.

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.

R2 LAN has a Record Management program that oversees record retention period for information. R2 Transit Subsidy System is EPA Schedule 1005, item b, which has a 6 year retention. R2 Telework is EPA Schedule 0039.

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 of having information retained beyond the length of time required.

Mitigation:

Region 2 has a Record Management Policy in place. Record control schedule is followed.

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.
Not applicable

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

4.4 Does the agreement place limitations on re-dissemination?
Not applicable

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. There is no information sharing.

Mitigation:

None.

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?

Region 2 LAN stores information in electronic files and does not take action on the information.

PII collection in these applications (Telework and Transit Subsidy) are used for the purpose granting telework and processing transit reimbursement. The information are reviewed and validated by the supervisors to ensure the use is in accordance with stated practices.

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

Users of the EPA system take the information security and privacy awareness training annually.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

The risk may be audit not being conducted properly.

Mitigation:

Region 2 has a review process in place that all data are accounted for.

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.

Region 2 LAN is used to store information in electronic files. The system does not take action on the information. Region 2 LAN is only for storage and it is the responsibility of the source system to ensure information is used for the reason for collection.

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 system is a local area network and electronic files may be stored on the network drives. By design the files are not retrievable by identifiers. Information is retrieved by file name not by PII.

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

No SORN is 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:

The risk that information is not handled in accordance with the uses describe above.

Mitigation:

Region 2 has audit logs that are reviewed to ensure information is handled properly 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 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: