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: Region 10 LAN	**System Owner: James Tyree**
Preparer: Jennifer Wolfe and James Tyree	**Office: Mission Support Division\Information Services Branch**
Date: 5/14/2024	**Phone: 206-553-1777**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s): Region 10 LAN GSS is in O&M stage.	
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:

The Region 10 Local Area Network (R10 LAN) is a general support system (GSS) providing the Information Technology (IT) infrastructure for Region 10. This includes hardware, software, applications, communications, network services (file/print/internet/intranet access) to support mission and daily operations within Region 10. EPA's Pacific Northwest Regional Office covers Alaska, Idaho, Oregon, Washington and 271 Tribal Nations. Environmental focus areas include air quality, ecosystems, Superfund, water quality and waste and chemical management. Information that is processed on or through can include virtually every type of information that EPA Region 10 employees create, use, store, maintain, disseminate, disclose, and dispose of in support of its mission. The components of the R10 LAN GSS make up the fundamental hardware and software that provide connectivity, security, storage, communications, Internet access, and data

access. The GSS includes client devices through which staff conducts their daily work. The R10 LAN GSS does not collect PII.

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?

The Privacy Act
The Freedom of Information Act
Electronic Government Act
EPA Privacy Act Regulations
Paperwork Reduction Act
Rehabilitation Act
Clean Air Act
Clean Water Act
Toxic Substances Control Act
Solid Waste Disposal Act
Safe Drinking Water Act
Comprehensive Environmental Response, Compensation, and Liability Act
Resource Conservation and Recovery Act Compensation and Liability Act
Oil Pollution Act
Emergency Planning and Community Right to Know Act
Residential Lead-Based Paint Hazard Reduction Act
Lead-Based Paint Poisoning Prevention in Certain Residential Structures Lead Renovation, Repair and Painting Program
National Environmental Policy Act
Federal Insecticide, Fungicide, and Rodenticide Act
Telework Enhancement Act
Federal Acquisitions Regulations
Federal Information Technology and Acquisitions Reform Act

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. The ATO for R10 LAN GSS expiration is August 1, 2025.

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 R10 LAN GSS does not collect PII data elements. R10 LAN GSS provides data storage and client devices, PII data elements may be stored on network storage or client devices by Region 10 employees.

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

R10 LAN GSS is not collecting PII data elements. The system is used to store the information in electronic data files created by Region 10 employees.

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.

Employees are responsible for their data. Employees are to manage their records according to records management requirements. Employees must complete annual Information Security and Privacy Training, Records Management training, and Controlled Unclassified Information Training. ISO and R10 Training Officer coordinates, monitors, and ensures employees have completed the mandatory training courses. Compliance to complete mandatory training in the allowed timeframe will result in an elevated awareness at the SIO level and employee will lose network access. Any new Region 10 systems or applications will undergo a review via the Agency Privacy process to ensure PII data is to be or not to be collected and Region 10 does not collect PII at this time.

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.

Privacy Risk:

Employees may store PII and other sensitive information on the R10 LAN GSS.

Mitigation:

Implementing required security and privacy controls in NIST SP 800-53, annual system assessments, and continuous monitoring of the system. R10 ISB procedures include daily, weekly, and monthly reviews of system logs. Employees are provided an autogenerated email if they have items that are saved to their OneDrive which contains potential PII data. ISO and R10 Training Officer coordinates, monitors, and ensures employees have completed the annual mandatory training courses. Compliance to complete mandatory training in the allowed timeframe will result in an elevated awareness at the SIO level and employee will lose network access. Employees who are leaving the Agency, transferring to another organization, or transferring to another organization outside of Region 10 are to follow the off-boarding policy and complete a records management checklist for separation that is signed by their supervisor and by R10 Records Liaison Officer prior to last day.

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. Region 10 GSS has different access control levels and are set based on roles and responsibilities. Access control levels to network storage and client devices include user, desktop and server administrator. For data stored on local network storage, permissions are set using security groups in Active Directory (limited to those with a need to access the files as applicable). Region 10 AD administrator manages access via Active Directory and Group Policy. Region 10 utilizes ServiceNow tickets for managing provisioning or deprovisioning of users, with tickets labeled "User Management Requests" including setting access control levels.

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

CIO 2150-P-01.3 Information Security – Access Control Procedure; Region 10 utilizes ServiceNow tickets for managing provisioning or deprovisioning of users, with tickets labelled "User Management Requests" including setting access control levels. For elevated account privileges, there is an Agency procedure to request accounts, and all accounts are reviewed annually by local IMO.

3.3 Are there other components with assigned roles and responsibilities within the system?

There are no additional components than what is reflected in Section 3.1.

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?

Region 10 employees (Federal, Contractor, SEE, interns) are granted access to files and folders on network storage based on roles and responsibilities following clearance from Physical Security Branch. Access is granted using security groups in Active Directory and set by Region 10 system administrators, who have access to all network storage. Elevated privileged accounts are reviewed annually. Existing contracts supporting Region 10 include: 68HE0920D0006: 68HE0720F0071 (RITTS – R10 Task Order – Veracity Consulting).

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.

The R10 LAN GSS is not a recordkeeping system and does not automatically delete or remove information. Data and information on the R10 LAN GSS that meets the definition of a record should be saved by the data owner to the agency recordkeeping system per applicable records control schedules.

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:

Employees may store PII and other sensitive information on the R10 LAN GSS. It is not a record keeping system and data\information is stored until the data owner removes it. The risk is when information is not managed timely or appropriately by employee.

Mitigation:

Implementing required security controls in NIST SP 800-53, annual system assessments, and continuous monitoring of the system. R10 ISB procedures include daily, weekly, and monthly reviews of system logs. Employees are provided an autogenerated email if they have items that are saved to their OneDrive which contains potential PII data. ISO and R10 Training Officer coordinates, monitors, and ensures employees have completed the annual mandatory training courses. Compliance to complete mandatory training in the allowed timeframe will result in an elevated awareness at the SIO level and employee will lose network access. Employees who are leaving the Agency, transferring to another organization, or transferring

to another organization outside of Region 10, are to follow the off-boarding policy and complete a records management checklist for separation that is signed by their supervisor and by R10 Records Liaison Officer prior to last day. For employees who did not complete the process, responsibility shifts to their immediate supervisor. Completion is certified by the Records Liaison Officer.

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:

Not Applicable.

Mitigation:

Not Applicable.

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?

Region 10 ensures GSS accessibility and operational status while adhering to CIO 2150-P-03.4 Information Security – Audit and Accountability Procedures. ISO is required to record a monthly attestation that all vulnerability reports are reviewed.

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

All Region 10 employees must complete annual Information Security and Privacy Training, Records Management Training, and Controlled Unclassified Information Training. ISO and R10 Training Officer coordinates and monitors and ensures employees have completed the mandatory training courses.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Users could inadvertently store and therefore share PII. A secondary risk is failure to audit and account for information use.

Mitigation:

Annual mandatory training, reminders regarding privacy and PII in MSD updates, and through various management and staff forums including the Executive Team, Monthly Managers Forum, weekly Deputies Meeting and Region 10 All Staffs. FOIA responses are reviewed and redacted where needed.

Implementing required security controls in NIST SP 800-53, annual system assessments, and continuous monitoring of the system. R10 ISB procedures include daily, weekly, and monthly reviews of system logs. Employees are provided an autogenerated email if they have items that are saved to their OneDrive which contains potential PII data.

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 R10 LAN GSS provides storage, accessibility, and control-of-access to Region 10 generated electronic data. It is not a system for records. This system does not use personal identifiers to retrieve information. The system does not collect PII information and does not utilize PII data or information.

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.*)

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 R10 LAN GSS is not a system of records, GSS is not intended to be used to search for information using an individual's PII. GSS is not used to officially collect PII.

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:

Users could inadvertently share data containing PII.

Mitigation:

All Region 10 employees must complete annual Information Security and Privacy Training, Records Management Training, and Controlled Unclassified Information Training. ISO and R10 Training Officer coordinates and monitors and ensures employees have completed the mandatory training courses.

Annual mandatory training, reminders regarding privacy and PII in MSD updates, and through various management and staff forums including the Executive Team, Monthly Managers Forum, weekly Deputies Meeting and Region 10 All Staffs. FOIA responses are reviewed and redacted where needed.

Implementing required security controls in NIST SP 800-53, annual system assessments, and continuous monitoring of the system. R10 ISB procedures include daily, weekly, and monthly reviews of system logs. Employees are provided an autogenerated email if they have items that are saved to their OneDrive which contains potential PII data.

***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

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: