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 5 Local Area Network (LAN) General Support System (GSS)	**System Owner: Aldwin Jereza**
Preparer: Michael Otaru	**Office: Region 5**
Date: 03/13/2024	**Phone: 312-886-2911**
Reason for Submittal: New PIA____ Revised PIA_x___ 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:

Region 5 Local Area Network (LAN) General Support System (GSS) provides the Information Technology (IT) infrastructure and support for Region 5's software, hardware including servers, computing equipment, internet, and applications. The network infrastructure processes information collected, maintained, and disseminated in furtherance of Region 5's mission, management, and administration. The following offices make up Region 5: Office of the Regional Administrator, Air and Radiation Division, Enforcement and Compliance Assurance Division, Great Lakes National Program Office, Laboratory Services and Applied Science Division, Land, Chemicals and Redevelopment Division, Superfund and Emergency Management Division, Water Division, Mission Support Division, and Office of Regional Counsel.

The types of information on the network drives include information received pursuant to the Clean Air

Act, Resource Conservation and Recovery Act, Compensation and Liability Act (Superfund), the Oil Pollution Act, the Emergency Planning and Community Right to Know Act, Safe Drinking Water Act, and the Marine Protection, Research and Sanctuaries Act, etc. These records may contain personally identifiable information about members of the public, including personal contact information, dates of birth, and residential address. Additionally, these records may contain sensitive personally identifiable information (SPII) about members of the public such as social security numbers (SSN). Although SSN is not typically collected or received in Region 5's matters, the Mission Support Division's network drives may contain SPII necessary for human resources matters, etc.

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?

Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C.9660.

Clean Air Act, 42 U.S.C. 7403.

Telework Enhancement Act of 2010, Public Law 111 – 292.

Toxic Substances Control Act, 15 U.S.C. 2609.

Solid Waste Disposal Act, 42 U.S.C. 6901 et seq.

Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. 9660.
1.2 Resource Conservation and Recovery Act
Compensation and Liability Act (Superfund)
Oil Pollution Act
Emergency Planning and Community Right to Know Act
Great Lakes Legacy Act, Safe Drinking Water Act
Marine Protection, Research and Sanctuaries 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 R05LAN GSS System Security Plan is updated and reviewed according to the Agency continuous monitoring plan.

Yes, the system was issued an Authorization-to-Operate (ATO) which expires in August 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.

No Information Collection Request (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, the data will not be maintained or stored in the Cloud.

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).

GSS is not a system that actively collects PII from individuals. It serves as a system infrastructure to house data such as network drives. The possible PII that Region 5 personnel could store on their network drives are contact information, dates of birth, and residential address about members of the public. Additionally, these drives may contain SPII about members of the public such as social security numbers (SSN). Although SSN is not typically collected or received in Region 5's matters, the Mission Support Division's network drives may contain SPII necessary for human resources matters, etc.

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

PII data elements are not directly collected by R05LAN. Sources of incidental PII data elements that can be found on the network include, systems internal to the EPA (e.g. Employee Express, People Plus)

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, the system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Data accuracy for each system is covered by the respective PIAs.

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:

There is a risk that Region 5 LAN GSS may temporarily display inaccurate data due to inaccuracies in underlying source.

Mitigation:

The risk is mitigated by the data being self-reported, and privacy act notices are provided on all EPA forms which address procedures for correcting 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?

Yes. R05LAN has access control levels within the system, enforced via Microsoft Active Directory user access configurations. Employees are granted least privilege to the network, based on access control levels, which are standard and privileged (desktop/servers admins) users.

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

R05LAN access controls are documented within the Access Control (AC) family of security controls within the R05LAN GSS System Security Plan maintained in EPA's system repository XACTA.

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

No, there are no other components are assigned roles and responsibilities within the system.

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?

The information is only accessible to authorized Region 5 employees.

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.

R05LAN does not automatically collect PII. PII information on the network is incidental and not intended for retention aligning with EPA Records Schedule No. 0008 Nonrecords such as convenience copies, working papers and drafts, etc. Information processed as part of official duties is intended to be stored in specific systems which are covered by individual PIAs and record schedules. Personal information stored by individual employees for their personal use is not governed by EPA records retention schedules. Employees are required to complete annual mandatory records retention/schedule training in EPA's FedTalent and adhere to applicable policies and guidelines.

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:

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule.

Mitigation:

R05 LAN GSS maintains all records with PII in accordance with applicable records retention or disposition schedules approved by NARA or based on the need and relevancy of the data in the support of the Region 5 mission. Some records are maintained as permanent records due to their continuing historical value; all other temporary records are disposed of in accordance with approved records schedules.

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 information is shared outside of EPA.

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 external 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 as stated in Section 6.1?

Region 5 LAN stores information in electronic files and does not act on the information. PII collected/processed by applications residing in Region 5, used for the purposes as intended. Region 05 LAN relies on the user training to ensure the information is used in accordance with the intended purpose. In the event an alert/evidence of data misuse is reported, a security incident is generated, and the Region 5 Security team works with the Region 5 Liaison Privacy Officer (R5 LPO) to assess the scope of damage and acts to take corrective actions.

The Region 5 Liaison Privacy Officer (R5 LPO) and the EPA National Privacy Program (NPP) also conduct annual data-calls/checks to ensure:

1. the PII data being collected, is used for the intended purposes, and
2. the applications collect the least amount of PII data elements to meet the stated purpose.

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

R05LAN users are required to take the annual Information Security and Privacy

Awareness (ISPAT) training. The training course instructs personnel on how to properly handle and secure PII information, and what actions to take in the event of a breach or unauthorized disclosure.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Region 5 employees may misuse and inappropriately disseminate information.

Mitigation:

EPA require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. EPA employee assigned to maintain the EPA systems have job duties that require them to design, develop, and optimize the system within the security accreditation environment. Furthermore, each employee is required to undergo annual security awareness training that addresses his or her duties and responsibilities to protect the 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.

R05LAN is used to store information in electronic files, and the system does not act on the information. It is the responsibility of the source system and application users to ensure the information is used for the purpose it was collected.

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.*)

R05LAN is a Local Area Network, and electronic files may be stored on the network drives or servers. By design the information is only retrievable by file name.

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?

Not applicable. No evaluation has been conducted on the potential effect of the privacy of

individuals because R05LAN does not retrieved information by a personal identifier, so 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:

There is a risk that a user may access information in Region 5 LAN GSS that he or she otherwise would not be able to view in the source systems.

Mitigation:

Region 5 LAN GSS is only available to authorized users who have been granted the appropriate privileges to access data from the connected IT system systems.

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

7.3 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?

7.4 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: