R EPA 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 4 LAN	
Preparer: Danna Mingo	**Office: MSD-ISMB-ITSS**
Date: February 29, 2024	**System Owner: Patrick Stone** **Phone: 404-562-8003**
Reason for Submittal: New PIA____ Revised PIA____ Annual Review__X_ 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:

The Region Local Area Network (LAN) General Support System (GSS), also known as R4 GSS LAN is a collection of platforms and systems that form a networked infrastructure to support data processing needs of EPA Region 4.

The R4 GSS LAN is used by EPA Region 4 employees and contractors. It is the infrastructure required to support mission functionality including network and security devices, file servers, workstations, printers, etc. The Region 4 GSS LAN is not a system of records. It does not collect PII, but it does provide the framework for other EPA Region 4 applications and systems that are responsible for PII. These systems

that collect PII using the R4 GSS LAN infrastructure are covered by their own separate PIAs.

The R4 GSS LAN covers all Information Technology (IT) infrastructure, which includes hardware, software, applications, databases, communications and Internet access to support mission and daily operations within EPA Region 4. As a result, the information that is processed on or through the R4 GSS LAN can include virtually every type of information that EPA Region 4 creates, collects, uses, stores, maintains, disseminates, discloses and disposes of in support of its mission, which is to protect human health and the environment. The components of the R4 GSS LAN make up the fundamental hardware and software that provide connectivity, security, storage, communications, Internet access, and data access. The R4 GSS LAN includes client devices through which staff conduct daily work and include central data storage and management devices.

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 legal authorities and/or Executive Orders are associated with the following disciplines: Air, Superfund, and Water. The following divisions are supported by the Region 4 LAN: Criminal Investigation Division; Regional Administrator's Office; Mission Support Division; Outreach & External Engagement Office; Press and Information; Office of Congressional and Intergovernmental Affairs; Air and Radiation Division; Regional Counsel; Land, Chemicals and Redevelopment Division; Laboratory Services & Applied Science; Superfund & Emergency Management Division and Water Division.

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?

The system has a security plan and is in the process of obtaining a renewal of the existing ATO which is scheduled to expire October 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?

Yes. This information system does store data on EPA servers located within the physical and logical boundaries of Region 4. Backup systems are located within the physical and logical boundaries of the EPA. However, we do utilize one cloud-based service, EQuIS online, which is Saas (Software as a Service) utilized by Superfund.

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 Region 4 GSS LAN is not a system of records and it does not collect PII, but it does provide the framework for other EPA Region 4 applications and systems that are responsible for PII. These systems that collect PII using the R4 GSS LAN infrastructure are covered by their own separate PIAs.

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

The system does not collect PII however, it is the infrastructure that supports the PII collected in other applications and systems.

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, specific systems hosted on this information system use data from public sources. This is primarily Geographic Information Systems and chemical data which is used for scientific analysis/modeling and enforcement actions.

2.4 Discuss how accuracy of the data is ensured.

Data accuracy for each specific system is covered by the respective PIAs. The Region 4 GSS LAN contains incidental PII and no coordinated efforts are made to review the data or ensure accuracy.

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 individual systems with the R4 GSS LAN have individual privacy controls which include limiting access (placing the records under lock and key and limiting access to named individuals). The incidental PII that accumulates on the system benefits from the protections offered to the GSS

LAN in general. This includes segregated file systems on the network that limit access, multi-factor authentication to gain access to the LAN in general, anti-virus software, active maintenance efforts by the Region 4 and National system administrators and desktop support teams.

The greatest threat to the incidental data is accidental/malicious disclosure. The greatest vulnerability is employee practices. Sensitive information stored on shared drives, for example, is placed at greater risk. Physical access to R4's offices requires visitors to be physically escorted. Facility security is controlled via electronic card access (PIV).

Mitigation:

Mitigation of the employee habit vulnerability is being addressed in multiple fashions. Region 4 has migrated to a system of redirected drives which place our files on the National OneDrive setup. Employees are subject to Information Systems Rules of Behavior. Annual employee training is mandatory and addresses security and privacy concerns and practices. Active anti-intrusion efforts by HQ and Region 4 seek to prevent bad actors from gaining access to the incidental 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?

All individual systems have access control mechanisms in place to restrict access to designated personnel. The incidental information within the Region 4 GSS LAN is protected from external intrusion by the EPA network and firewall, all communications between the Region 4 GSS LAN and the exterior internet pass through the Agency firewall. Internal controls include the use of multi-factor authentication to gain access to the Region 4 GSS LAN and compartmentalization of data within the LAN to minimize individual employee access to data. Examples include: Active Directory (AD) user groups to control access to specific data storage containers, personal email accounts.

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

Access controls for the Region 4 GSS LAN are outlined in the Information Security Access Controls Policy and System Security Plan. As required by NIST, the data is reported and documented in Automated System Security Evaluation and Remediation Tracking (ASSERT).

Pursuant to the Region 4 System Security Plan, initial access to the Region 4 GSS LAN is controlled primarily via the hiring process which requires background checks. Individual employees are granted the least level of access required by their position. Monthly reviews of special access groups are performed and employee access is reviewed when employee actions (moves, transfers) are reported to the Information Technology (IT) program by Human Resources. The Records Liaison Officer works collaboratively with IT to ensure that user accounts are

disabled timely (normally within thirty (30) days) upon the departure of EPA staff or contractors and ensures the proper security or disposal of all electronic records.

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

Yes. The Region 4 GSS LAN hosts multiple individual systems which control access with assigned roles. Those systems containing PII are documented in individual PIAs.

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?

Incidental PII contained on the Region 4 GSS LAN is confined to internal systems users (EPA employees and contractors) by the controls which limit access to the information system. All Region 4 contracts adhere to Agency and Federal requirements and contain the appropriate 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.

Because information on the Region 4 GSS LAN is incidental and not intended for retention, there is no record control schedule number. However, there is the potential for PII to reside within the R4 GSS LAN as the result of being typed into the text of an email message or attached to an email message sent or received by a R4 employee or contractor or by being downloaded from another system and saved by that system's user to his or her EPA-issued personal computer. Some examples of PII that could be stored or transmitted using the LAN include travel, payroll, time and attendance, and other agency personnel records containing PII pertaining to employees and contractors; agency program records containing PII pertaining to members of the public; and employees and contractors personal records (non-agency records).

Some of the systems that do reside on or interface the Region 4 GSS LAN and their accompanying record schedules are PPL (0300), MANS/COOP (1049, 0740, 0757, 0090), Transit (1049/0090), Employee Performance File Systems (0107), Administrative Grievance, Disciplinary Adverse Action Files (0564), Outside Activities (1033), EPAYS (0573), Medical Surveillance (0023), and Fleet (0090).

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. Each LAN account holder controls the retention and deletion of information in his or her account while the account is active. A user's account on the LAN is disabled immediately after the employee or contractor leaves EPA Region 4.

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:

Inadvertent or unintended internal access to incidental data is the greatest vulnerability in this case.

Mitigation:

Region 4 seeks to mitigate this risk by adhering to Agency practices and standards. Personnel are required to complete security training before being given significant network access. Employees are provided with data storage options which limit the pool of personnel who can see the data. Background checks are administered to all employees and contractors and annual training is given to those that require enhanced access to the LAN or applications on it.

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. Data sharing is internal. The Region 4 GSS LAN is a data hosting system. Information sharing is performed by specific systems, notably the Region 4 webpage, which operates as a subset of the national EPA webpage. Data sharing by individual systems that store PII is documented in their individual PIAs. The LAN system manager and system administrators are responsible for ensuring proper agency security procedures are adhered to for the R4 GSS LAN.

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

This is not applicable to the R4 GSS LAN. It is not a *system* designed to collect and share data. Data sharing is done by individual systems on the LAN as detailed in individual PIAs.

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?

The system does not review and/or approve information sharing agreements. Data sharing is accomplished by specific systems on the R4 LAN. If it was necessary to share data, a new

sub-system would be created (and a PTA filed) to accomplish that specific function. Region 4 has an incipient or nascent Data Management committee to which questions regarding data sharing can be addressed. Implementing a new system would require a general IT approval going through our weekly change control process.

4.4 Does the agreement place limitations on re-dissemination?

The data is for internal EPA use.

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:

The greatest risk to this information is misuse of information by employees, e.g. sharing information with personnel who do not have approved access to the information.

Mitigation:

Sensitive information can flow out of the Agency through email, printed copies, instant messaging or by people simply talking about things they should keep to themselves. Security policy and technology must be combined to mitigate the risk of disclosure outside the Agency.

Since insiders (employees/contractors) are typically subject to very few controls, we tend to rely on trust rather than technical or procedural countermeasures to manage or control external access. When transmitting information, the name, department and email of the recipient is confirmed. The personal information is attached to the email and saved as "read only" with encryption or electronic document password protection.

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?

The Region 4 GSS LAN relies on user training to ensure that information is used in accordance with the stated practices. System administrators, network operators, and system support staff are alert to evidence of data misuse and alert the greater Region 4 IT team when such evidence is discovered. The IT team assesses these incidents and acts to take corrective actions.

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

Region 4 relies upon the national Information Security and Privacy Awareness training

delivered annually by the Agency.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Unrecorded data changes.

Mitigation:

This risk is mitigated by the Active Directory control which prevents concurrent access to data files and records the last date changes were made.

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 Region 4 GSS LAN exists to host systems which store and process PII data and is used to host applications that can be used to process data from these systems and to temporarily store those processing files.

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 Region 4 GSS LAN is not a system of records. It does not actively collect or retrieve PII information.

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:

Lack of familiarity with Government practices regarding PII may lead individual employees to create data collections containing PII which are not reported and adequately protected.

Mitigation:

Region 4 has prepared and implemented a plan which expands upon the annual, national requirement to report any systems which contain SSNs. All program managers surveyed their staff to identify all data collections (MS Access files, Excel files, SQL Express files, and etc…) which contain ANY PII. Steps have been taken to ensure that any "new" systems identified containing ANY PII will file a PTA and take adequate protection steps

*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.

This system does not collect information directly from an individual.

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?

N/A

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:

N / A

Mitigation:

N/A

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?

Procedures to allow individuals to access their information is maintain in the specific system of record notice associated with the applicable application or system that collects the information.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Procedures to allow individuals to correct inaccurate or erroneous information is maintain in the specific system of record notice associated with the applicable application or system that collects the 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:

N / A

Mitigation:

N/A