EPA United States
Environmental Protection
Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: R08 GSS LAN	
Preparer: John A. Jordan II	**Office: Region 08, MSD-IMB**
Date: 03/18/2020	**Phone: 303-312-7072**
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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f)</u>.

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A)</u> (pgs. 44-45).

Provide a general description/overview and purpose of the system:

Region 8 Local Area Network (LAN) General Support System (GSS), also known as R08 GSS LAN is a collection of platforms and systems that form a networked infrastructure to support data processing needs of EPA Region 8.

R08 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 8. As a result, the information that is processed on or through can include virtually every type of information that EPA Region 8 creates, collects, uses, stores, maintains, disseminates, discloses and disposes of in support of its mission, which is to protect human health and environment. The components of the R08 GSS LAN 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 conduct daily work, and also 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?

Section 2 of the E-Government Act of 2002 (Pub. L. 107-347, 44 U.S.C. 3601 n.)

Section 2 of the Paperwork Reduction Act of 1995 (Pub. L. 104-13, 44 U.S.C. 3501)

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?

This PIA is for the information system which Region 08 uses to support specific systems which collect and process PII. The system has a security plan and is in the process of obtaining a renewal of the existing ATO which was scheduled to expire in September, 2019.

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. This information system stores data on EPA severs located within the physical and logical boundaries of Region 08. Backup systems are located within the physical and logical boundaries of the EPA. No cloud services external to the EPA network are used.

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 information stored on and transmitted with this information system is covered by individual PIIs detailing each of the specific systems involved. In addition, this information system has been determined to contain random PII. This PII is composed of miscellaneous output from systems both internal and external to the EPA and consists of medical, personal, and financial information incidental to EPA/Regional operations. Examples include: Pay Records downloaded by individual employees, medical records (appointments, medical information), personal contacts, and individual SSNs.

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

This information system does not collect data. The sources of the information that can be found on the system include systems internal to the EPA (e.g. Employee Express, People Plus) and systems external to the EPA (e.g. credit reporting bureaus, personal emails, and etc).

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 08 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 R8 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, two factor authentication to gain access to the LAN in general, anti-virus software, active maintenance efforts by the Region 8 and National system administrators and desktop support teams.

The greatest threat to the incidental data is accidental/malicious disclosure. The greatest vulnerability is employee habits. Sensitive information stored on shared drives, for example, is placed at greater risk.

Mitigation:

Mitigation of the employee habit vulnerability is being addressed in multiple fashions. Region 8 has migrated to a system of redirected drives which place our files on the National OneDrive setup. Employee education is mandatory on an annual basis and addresses security and privacy concerns and practices. Active anti-intrusion efforts by HQ and Region 8 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 08 GSS LAN is protected from external intrusion by the EPA network and firewall, all communications between the Region 08 GSS LAN and the exterior internet pass through the Agency firewall. Internal controls include the use of two factor authentication to gain access to the Region 08 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 What procedures are in place to determine which users may access the information and how does the system determine who has access?

Per the Region 8 System Security Plan, initial access to the Region 08 GSS LAN is controlled primarily via the hiring process which includes background checks. Individual employees are granted the least level of access which their position requires. Monthly reviews of special access groups are conducted and employee access is reviewed when employee actions (moves, transfers) are reported to the Information Technology program by Human Resources.

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

Yes. The Region 08 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 08 GSS LAN is confined to internal systems users (EPA employees and contractors) by the controls which limit access to the information system. All Region 08 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.

Information on the Region 08 GSS LAN is incidental and not intended for retention. 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.

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:

Unintended internal access to incidental data is the greatest vulnerability in this case.

Mitigation:

Region 8 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 performed and annual training 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.

The Region 08 GSS LAN is a data hosting system. Information sharing is performed by specific systems, notably the Region 08 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.

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

This is not applicable to the R8 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 their 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. Data sharing is accomplished by specific systems on the R8 GSS 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 8 has a 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 employees misuse of information. E.G. Sharing information with personnel who do not have approved access to the information.

Mitigation:

Region mitigates this risk by limiting staff access to data sets and requiring and providing annual training on privacy procedures for employees.

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?

The Region 08 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 08 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 08 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 prevent concurrent access to data files and record 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 08 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.)*

The Region 08 GSS LAN is not designed to process PII information. It is possible that individual files may be created by employees which contain PII in their file name. This would enable the file to be retrieved by looking for the PII. Region 8 has no way to prevent this from happening, but individual annual privacy training makes it clear that protecting PII is an Agency priority and discourages this practice. Files which are datasets are required to be described in an individual PIA which would be attached to this system PIA.

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

Region 8 has 2 SORNs associated with specific sub-systems associated with the R8 GSS LAN. These systems have individual PIAs which are attached.

The Libby Asbestos Exposure data set is associated with SORN EPA-48.

The Medical Surveillance/Reasonable Accommodation data set is associated with SORN

EPA-70.

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>:

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.

<u>Mitigation</u>:

Region 8 is preparing to implement a plan which expands upon the annual, national requirement to report any systems which contain SSNs. It is our intention to have program managers survey their staff to identify all data collections (MS Access files, Excel files, SQL Express files, and etc…) which contain ANY PII. We will then act to ensure these systems 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.

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 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

<u>Mitigation</u>:

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: