



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: R3 LAN\GSS	System Owner: Philip Workman
Preparer: Robert Siliato, ISO, LPO	Office: R03-MSD-OSB-IIMS
Date: 2/26/2026	Phone: 215-814-5361
Reason for Submittal: New PIA _____ Revised PIA ___ Annual Review (X) 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 <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) (pgs. 44-45)</u>.	

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

The Region 3 network is a General Support System (GSS) that provides access to local area network (LAN) services and wide area network (WAN) access to both the EPA national network and the internet. The R3 LAN is a communications system, not a system of records. The Region 3 network's primary office is in Philadelphia, with remote locations in the Environmental Science Center in Fort Meade, Maryland, the Chesapeake Bay Office in Annapolis Maryland, and the remote laboratory in Wheeling, West Virginia. The system also provides some Geographical Information System (GIS) support for specialized applications. The Region has an operational hot site at Fort Meade, MD which has operational file and print servers and a replication capability to provide emergency backup for the Philadelphia office. The R3 LAN does not actively collect information; it is used by EPA employees and authorized contractors in the

course of conducting official EPA business to store and communicate information. R3 users also have limited personal use of authorized equipment attached to the R3 LAN.

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 (CERLA) 42 U.S.C.9660.
- 40 CFR Part 745 – Lead-Based Paint Poisoning Prevention in Certain Residential Structures
- 5 U.S.C. 5101 et seq.; 5 U.S.C. 6301 et seq.; 5 U.S.C. 6311; 5 U.S.C. 522a.
- Beaches Environmental Assessment and Coastal Health (BEACH) Act
- Chemical Safety Information, Site Security and Fuels Regulatory Relief Act
- Clean Air Act 42 U.S.C. § 7401 et seq 1970
- Clean Water Act (CWA)
- Compensation and Liability Act (Superfund)
- Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) of 1980 42 U.S.C § 9601 et seq.
- EPA Privacy Act Regulations, 40 CFR Part 16
- Emergency Planning and Community Right-to-Know Act (EPCRA)
- Endangered Species Act (ESA)
- Energy Independence and Security Act (EISA)
- Energy Policy Act
- EO 12898: Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations
- EO 13045: Protection of Children from Environmental Health Risks and Safety Risks
- EO 13211: Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use
- Solid Waste Disposal Act, 42 U.S.C. 6901 et seq.
- Federal Insecticide, Fungicide, and Rodenticide Act 7 U.S.C. §136 et seq.
- Food Quality Protection Act (FQPA)
- Marine Protection, Research and Sanctuaries Act
- Pollution Prevention Act
- Oil Pollution Act
- Residential Lead-Based Paint Hazard Reduction Act of 1992
- Resource Conservation and Recovery Act
- Safe Drinking Water Act (SDWA) 42 U.S.C § 300f et seq. 1974
- Telework Enhancement Act of 2010, Public Law 111 – 292.
- Toxic Substances Control Act (TSCA)

CUI//ISVI

- 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 the R3 LAN|GSS expires January 8, 2027

- 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?**

The R3 GSS is not provided by a CSP.

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).**

R3 GSS: The R3 GSS\LAN does not specifically collect PII information. R3 GSS\LAN serves as a system infrastructure to house data such as network drives. R3 Employees have the capability to store EPA work related information on various servers or their agency issued laptops such as contact information, and residential address about members of the public. To get a better understanding of what users store on the network, we sent out a questionnaire asking if R3employees had collected or maintained PII, SPII on behalf of the EPA. Users have reported collecting the following:

1. Residential sampling agreements, results letters, well monitoring sampling, access agreements (Name, address, telephone number)
2. Private well monitoring data (name, phone number).
3. Site assessment activities (name address, phone, email, location of private wells)
4. *Sometimes* Elevated blood level (EBLL) medical data is sometimes received from health departments (general in nature, only says whether there have been any EBLL at the address they are inspecting.
5. PFAS (Polyfluoroalkyl Substances) well results (name, address)

CUI//ISVI

6. Private well and vapor intrusion sampling info (name and address)

The storage of this information could reside on various shared or locked network drives in various forms of documents such as but not limited to word documents, excel spreadsheets, and PDF's.

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

R3 GSS\LAN is not a system of records. To get a grasp of what users saved on the R3 network, we sent out a questionnaire. Responders to questionnaire reported pdf files, word docs, excel spreadsheets, email contact lists, iPhone contact lists for EPA internal information. The information collected was through verbal and electronic submission. This questionnaire was submitted to Deputy Division leaders and disseminated to the branch chief under their purview. Some chiefs answered for the whole branch while some individuals answered for themselves. This survey was sent out in trust that everyone answered the questionnaire truthfully and to the best of their knowledge. Not everyone in the region responded.

As a result, responders and leaders in management were told to remove any emergency contact lists or convenience copies of such from the R3 network since the decommissioning of an Emergency Contact Information System. *The ECIS no longer exists. All emergency contacts are now managed by the EPA's National Mass Alert Notification System (MANS) or through Human Resource personnel.*

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.

All R3 employees who maintain data are responsible and determines if the data is still relevant and accurate.

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 risk could be that PII potentially could be accessed without a need to know. SPII was previously disclosed to the R3 LPO and ISO and reported to be kept on several users' laptops as a convenient

copy of what was already in national system. User were told to remove that data.

Mitigation:

This has been mitigated by restricting access through the use of personal shares with individual access or group shares locked down with approved users with permission restrictions. The users were directed to delete all call down lists or convenience copies and cease to continue that practice.

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 R3 LAN\GSS is not a system of records. Each EPA employee and contractor is allowed access to his or her LAN account only. Shared folders and file storage drives are managed with group access and active directory security policies. Critical components of the LAN are accessed by the system administration group which manages user IDs and passwords, security settings, and patching/upgrades. The EPA Network is secured by a combination of firewalls, anti-virus controls, intrusion detection and prevention systems, network controls, access lists and account creation, policing and termination processes. Physical access to the system is restricted through security guards and access badges required to enter facility each EPA facility. EPA employees and contractors are subject to the EPA's National Rules of Behavior and receive annual security awareness training.

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

The system access control is documented in the SSP - NIST SSP for Region 3 LAN (R3 LAN).

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

Yes. There are instances where other members from other agencies can access the R3 network. Their access is limited to their role and responsibility and Active Directory (AD) controls.

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?

Contractors will have access and the appropriate clauses are in place. (Reference AR-3 in SSP)

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.

EPA/0089, Information Tracking Systems, broadly covers electronic databases. EPA/0089 directs IT/IM professionals to further identify the specific schedule covering a given database and to follow the instructions for disposition in that schedule.

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 risks associated with retaining data over a period of time is that the longer it is held, the greater the risk of it being compromised.

Mitigation: In order to protect privacy information that the agency is required to hold on the public, is to store data on isolated locations, such as personal shares (F: drives) and Office 365 OneDrive. If users are required to transport data, they must fill out a form and receive authorization. They must use an encrypted drive. They must only hold a local download for time specified in the authorization form.

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.

N/A

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?

CUI//ISVI

The system does not review or approve information sharing as it is not a system of records. If there is a such a need to review such documents, a request is sent to the SIO for approval. Approvals are granted only after a risk analysis is completed and any mitigation required to be put in place.

4.4 Does the agreement place limitations on re-dissemination?

N/A

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. Information is not shared externally.

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?

The R3 LAN\GSS is not a system of records. It is a Local Area Network consisting of file servers, print servers, storage servers, user laptops. Active Directory rights and restrictions are assigned to users and groups.

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

Users are required to take the mandatory annual Information Security and Privacy Awareness Training (ISPAT).

5.3 **Privacy Impact Analysis:** Related to Auditing and Accountability

Privacy Risk:

Users who do not have the proper training to protect PII are at risk of unauthorized disclosure and possible breach of data.

Mitigation:

Users must take the mandatory ISPAT or have their access blocked.

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 R3 GSS system is not a system of records. It is a general support system (GSS) that connects to the overall EPA network, providing primarily mail and file and print services for the organization at the office in Philadelphia, and remote locations in the Environmental Science Center in Fort Meade, Maryland, the Chesapeake Bay Office in Annapolis Maryland, and the remote laboratory in Wheeling, West Virginia. The system also provides some Geographical Information System (GIS) support for specialized applications. The Region has an operational hot site at Fort Meade, MD which has operational file and print servers and a replication capability to provide emergency backup for the Philadelphia office.

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 R3 GSS, is not a system or records and does not retrieve any information via personal identifiers.

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 R3 LAN\GSS is not a system of records. Previously a survey was sent out to regional users regarding a portion of the R3 GSS\LAN covered a portion of the PII was collected/maintained for the Emergency Contact Information System (ECIS) which was covered by EPA SORN-44.

The ECIS **has now been decommissioned** and the SORN only applied to that. Therefore EPA SORN-44 was removed from R3 GSS.

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

CUI//ISVI

accordance with the uses described above.

Privacy Risk:

At a minimum, the data could be misused.

Mitigation:

Ensuring the above controls are met and followed. Users are also required to take the annual ISPAT training and sign the rules of behavior. Because the LAN is not a system of records (and therefore not a source system), the LAN does not ensure data accuracy.

***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 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:

I attest as the Agency Privacy Officer that **Region 3 R3 LAN\GSS** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA