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: Region 3 LAN (GSS)	
Preparer: Robert Siliato	**Office: Region 3**
Date: 12/13/2019	**Phone: 215-814-5361**
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:

As part of our annual accreditation, Region 3 was noted for not conducting a PIA for the entire R3 GSS. This document is to meet that requirement.

The Region 3 network is a general support system, 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.

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?

Program Office determines the authority for collection of PII based on their mission.

Authority is reviewed and approved by Office of General Counsel (OGC).

The authority for collection is published in a System of Records Notice (SORN) in the Federal Register by the National Privacy Program.

United States Code

• The Privacy Act of 1974, 5 U.S.C. § 552a, as amended

• The Freedom of Information Act, 5 U.S.C. § 552, as amended

• The Electronic Government Act of 2002, 107-347,44 U.S.C. Ch 36

Code of Federal Regulations

• EPA Privacy Act Regulations, 40 CFR Part 16

Federal Register: January 4, 2006 (Volume 71, Number 2)

Privacy Policy EPA Privacy Policy

SORN Procedures for Preparing and Publishing Privacy Act Systems of Records Notices (PDF)

PA Request Procedure Processing Privacy Act Requests Procedure (PDF)

Procedures for Preparing Privacy Act Statements (PDF)

• General Awareness Training

• System Owners.

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 GSS\LAN expires Feb 27, 2021

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 has previously reported on the R3 ECIS (Emergency Contact Information System) which was covered under EPA SORN 44. Since that time, we were told that the ECIS falls under the MANS umbrella of coverage and reporting on that system is not a R3 responsibility.

The R3 GSS\LAN does not specifically collect PII information. R3 Employees have the capability to store EPA work related information on various servers or their agency issued laptops.

We sent out a questionnaire asking if R3employees had collected or maintained PII, SPII on behalf of the EPA. User's reported collecting the following:

Emergency contact lists (name, address, home phone or cell phone)

Residential sampling agreements, results letters, well monitoring sampling, access agreements (Name, address, telephone number)

Private well monitoring data (name, phone number).

Site assessment activities (name address, phone, email, location of private wells)

Sometimes Elevated blood level (EBLL) medical data is sometimes received from health departments (general in nature, only says whether or not there have been any EBLL at the address they are inspecting.

PFAS (Polyfluoroalkyl Substances) well results (name, address)

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

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

The term system does not really apply to the R3 GSS. 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 were told to remove any convenience copies from the R3 network if the information was already stored in a System of Records (SOR) or previously printed out and stored in a locked cabinet.

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 convivence 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 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?

Yes. User and Password authentication, multifactor authentication through smart cards, Active Directory and Windows permissions.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

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 clause 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.

Each system enforces their RCS associated with the data elements in it

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?

If there is a such a need to review it 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 in accordance with stated practices in this PIA (Section 6.1)?

We send out an annual survey to users to confirm their use and purpose of any PII they may retain. Users respond to the survey in a timely manner.

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

User's 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 discloser 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 system is a general support system, 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.*)

No, the system is General Support System and accesses information on a per individual basis and not by a personal identifier. ECIS is the only component of the R3 GSS that retrieved information by a personal identifier and is covered by its own SORN. The R3 GSS consist of over 50-70 servers, printers, over 1,000 EPA user machines, EPA issued iPhones, and other equipment such as video conferencing systems and wireless access points.

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

Currently a portion of the R3 GSS\LAN covers a portion of the PII that is collected/maintained for the Emergency Contact Information System (ECIS) which is covered by EPA SORN-44.

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:

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.

*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 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: