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 Roster.docx

System Name: Region 7 Local Area Network (R07LAN)		**System Owner: Randy Downs**	
Preparer: Randy Downs		**Office: Region 7**	
Date: 3/13/2024		**Phone: 913-551-7505**	
Reason for Submittal:			
New: ☐	Revised:☒	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: ☒	Rescindment/Decommission: ☐		
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 7 covers and serves Iowa, Kansas, Missouri, Nebraska, and nine Tribal Nations. EPA has established offices within Region 7 to reduce lead exposure by creating lead-safe environments and identifying and cleaning up lead-contaminated properties throughout the region. Region 7 is comprised of the following offices: Office of the Regional Administrator (ORA), Air and Radiation Division (ARD), Enforcement and Compliance Assurance Division (ECAD), Land, Chemicals and

Redevelopment Division (LCRD), Laboratory Services and Applied Science Division (LSASD), Mission Support Division (MSD), Office of Regional Counsel (ORC) Superfund and Emergency Management Division (SEMD), and the Water Division (WD).

The Region 7 Local Access Network (LAN) General Support System (GSS) provides the IT infrastructure, connectivity and central control of data processing, telecommunications, electronic mail, and internet functions to offices within Region 7. Region 7 LAN GSS is comprised of file servers, routers, switches, and infrastructures that provide Region 7 personnel voice/data, email, file sharing, development and collaboration services. It supports agency administrative functions, document storage and retrieval, emergency response, scientific calculations and modelling and geographic information system (GIS) modelling and graphing. It is also used to maintain regional programs environmental databases and an environmental sample analyses database.

Section 1. 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?

5 U.S.C. 5101 et seq.; 5 U.S.C. 6301 et seq.; 5 U.S.C. 6311; 5 U.S.C. 522a.

Title IV of Toxic Substances Control Act (TSCA)

Residential Lead-Based Paint Hazard Reduction Act of 1992

40 CFR Part 745 – Lead-Based Paint Poisoning Prevention in Certain Residential Structures

Lead Renovation, Repair and Painting Program (RRP) Rule: TSCA sections 402/404, Section 1018 of Title X, TSCA section 403

Clean Air Act 42 U.S.C. § 7401 et seq 1970

Safe Drinking Water Act (SDWA) 42 U.S.C § 300f et seq. 1974

Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) of 1980 42 U.S.C § 9601 et seq.

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 (ATO)? When does the ATO expire?

Yes, a system security plan has been completed. The current ATO expires 6/30/2024.

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.

No Information Collection Request is 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, data will not be maintained or stored in a cloud.

Section 2. 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).

Region 7 LAN GSS serves as a system infrastructure to house data such as network drives. The possible PII that Region 7 personnel could store on those 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), medical, and financial information. Although SSN, medical, and financial information is not typically collected or received in Region 7's matters, offices' 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?

Region 7 LAN system could potentially be used to view or maintain miscellaneous PII output from systems both internal and external to the EPA that consists of medical, personal, and financial information incidental to EPA/Regional operations.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

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

2.4 Discuss how accuracy of the data is ensured.

Region 7 LAN GSS depends on the accuracy and quality of information provided by other systems within Region 7. Any checks for data accuracy are performed in the underlying connected IT systems. If an end user determines that erroneous information is being stored by the connected IT systems, the user can correct the information by signing into the system via the application and correcting the erroneous data in accordance with established policy, processes, and training. If the user does not have update privileges, he or she may request that the change be made by notifying the appropriate data management staff, following the policies for data changes that are in effect for the system.

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:

There is a risk that Region 7 LAN GSS could potentially retrieve more information than required from the connected IT system which could result in accidental or malicious disclosure.

Mitigation:

Agency Data Loss Prevention (DLP) tools have been added to Microsoft Outlook, OneDrive, and Teams to prevent over collection of information.

Section 3. 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, Region 7 inherits access control levels from EPA Common Controls, Enterprise Identity Access Management (EIAM). See Region 7 LAN Xacta Control AC-2 (Account Management) for full details, control levels summarized here:

- Region 07 LAN utilizes individual user and privileged "dotted" accounts to support EPA mission business functions.
- Authorized users for Region 7 LAN are issued unique identifiers to create their EPA LAN account credentials. Group and role access have been identified as AD access groups in which membership to group grants privileges to specified file share.
- File share access is Access Based Enumeration (ABE) in which files are hidden from unauthorized users' view. Access privileges for each user account have been identified as Read-only unless Read/Write access is requested.

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

From Xacta Control AC-1 (Access Control Policy and Procedures): Region 7 inherits access controls from EPA Common Controls, Chief Information Officer (CIO) 2150-P-01.2. Office of Information Security and Privacy (OISP) notes The AC procedure is under Review. Plan of Action and Milestones (POAM)52 OISP is in place to track the remediation of this finding. The AC procedure will be updated after the National Institute of Standards and Technology

(NIST) 800-53 Revision 5 document is out to include the new NIST 800-53 Revision 5 requirements.

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

There are no other components with 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?

Only internal parties will have access to data/information in the system. An internal party is defined as those with an EPA LAN account and Personal Identity Verification (PIV) card and may include contractors. FAR 52.217-8 and 52.217.9 clauses are included in the contract. External parties do not have access to Region 7 LAN data.

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.

Region 7 LAN IT implementation records are covered under EPA records schedule 1012. All other program records stored on the regional network share drives are covered under the appropriate EPA subject schedules. Records related to LAN implementation and compliance are retained for 7 years per EPA records schedule 1012 item b (NARA Disposal Authority: DAA-0412-2013-0009-0002). Records related to routine LAN operations and maintenance are retained for 3 years per EPA records schedule 1012 item c (NARA Disposal Authority: DAA-0412-2013-0009-0003). Non-records and convenience copies are covered under EPA records schedule 0008 and subject to disposal immediately after determining if information is superseded, obsolete or no longer needed for reference. Personal files that do not relate to, or have an effect upon, the conduct of Agency business and are stored by individual employees for their personal use are covered under EPA records schedule 0999 and can be destroyed or removed at the owner’s discretion.

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:

Region 7 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 7 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. 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.

Information is not shared externally.

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

Information is not shared externally.

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?

Information is not shared externally.

4.4 Does the agreement place limitations on re-dissemination?

Information is not shared externally.

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. Information is not shared externally.

Section 5. 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?

Information Security and Privacy Awareness Training (ISPAT) training is required for all system users annually, and requires users acknowledge the National Rules of Behavior (NRoB) in using government systems.

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

General privacy training is given to all users on an annual basis via FedTalent's mandatory Information Security and Privacy Awareness Training (ISPAT) training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

Region 7 employees may misuse and inappropriately disseminate information.

Mitigation:

EPA require auditing capabilities that log the activity of each user in order 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. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

PII data elements that are stored, processed, or transferred via the Region 7 LAN are incidental to the system and limited to use by the individual for miscellaneous (personal, employment, financial, or medical) purposes.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☐ No: ☒ 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.

Information is retrieved 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?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

No evaluation has been conducted on the potential effect of the privacy of individuals because the because Region 7 GSS LAN does not collect 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 7 LAN GSS that he or she otherwise would not be able to view in the source systems.

Mitigation:

Region 7 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 National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

Click or tap here to enter text.

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:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.

Section 8. 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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver’s license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted.

Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

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

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA’s Privacy Act regulations at 40 CFR part 16.

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 Freedom of Information Act (FOIA).

Privacy Risk:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.