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: National Center for Radiation Field Operations LAN GSS	**System Owner: Andrea Stafford**
Preparer: Fernando Gomez	**Office: OAR-ORIA-NCRFO**
Date: 12/01/2020	**Phone: (702) 784-8222**
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 NCRFO LAN GSS includes the NCRFO EPA LAN (a segment of the EPA WAN) and NCRFO FieldOps LAN (a stand-alone analytic network).

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?

44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014

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?

SSP is complete. ATO expires 8/2021.

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?

No.

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 system primarily supports administrative and analytic functions of the National Center for Radiation Field Operations (NCRFO): NCRFO LAN administrative functions include documentation regarding purchasing, contracts, budget, and facility access. The system provides access to web applications supporting functions such as purchasing, time keeping, travel and hiring but does not operate those systems. Data entered web applications is stored on servers managed by the application host.

NCRFO LAN GSS does not host any public facing web applications or servers.

Facility access applications record the names of visitors who enter EPA facilities and secured areas and the time of access. Monthly reports are created for Office Directors to audit building access.

FieldOps LAN analytic functions include radiation measurements for environmental samples using handheld and mobile instruments, and reports to clients. Clients include EPA Regions, other Federal agencies, states, and tribes. NCRFO does not take or

exchange PII with clients. Only information necessary for analysis and reporting – location, time, weight, sample matrix, etc. – is collected by NCRFO. Quality assurance consists of verification (were all required sample variables reported) and validation (did variable limits make sense, were calculations correct, were instruments properly calibrated, etc.).

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

Data in the system is primarily documents generated locally in Agency approved Microsoft Office applications. The following types of information reside in the system:

- Contract specifications, work orders, costs, manpower requirements are provided by NCRFO. Proposals are submitted by bidders to specific EPA personnel.
- Purchasing specifications, bids, and cost data related to ordinary office expendables, new purchases and maintenance.
- Budget information is exchanged between NCRFO and EPA headquarters. This is a normal function of any business. It occurs within the EPA WAN according to established procedures – usually a data call request initiated by headquarters.
- QA and project plans for monitoring radiation in support of environmental justice programs, tribes, states, and federal agencies. Any PII is collected by supported entities and is not exchanged with NCRFO as it is irrelevant to analysis and measurement reporting.
- Radiation measurements from handheld and mobile response laboratory instruments in support of the field training and emergency response missions.

Data points collected that are required for the systems to operate are: User first and last names, usernames, position, and email addresses obtained via Active Directory, eBusiness, ASQ and other directories provided by the Agency. Yes it comes from Active Directory on the EPA LAN. These are the only data points used. Data used from EPA LAN Active Directory is used to populate/store in the FieldOps Active Directory and it is not stored in any other application/system

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.

The accuracy of business data is dependent on the department conducting the collection, such as OMS, and that office's vetting process as NCRFO does not collect any identifiable data itself.

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 first name, last name, username, position and email address which the system requires in order to operate could potentially expose government users to increased spam traffic and possible social engineering.

Mitigation:

The system uses least privilege and need-to-know controls in accessing the storage of business identification data obtained from Agency-provided resources.

All information on desktop and laptop computers across the GSS is encrypted using Microsoft BitLocker and access requires dual factor authentication. The information above is collected by specific individuals with responsibilities in the given area. All personnel have a personal network drive with access restricted solely to them. Directories on NCRFO file servers have restricted access as directed by NCRFO management specifically to limit access to necessary individuals.

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?

Data in the system is separated according to access control levels. Only persons who have necessity to access information have the necessary rights. Administrative data is available only to individuals with specific duties related to personnel, purchasing, budgets, and contracts. Center directors may be granted access as required according to specific needs. There is no public access to the NCRFO LAN GSS.

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

The System Security Plan (SSP) and Rules of Behavior contain the access controls that define policies and procedures for data access and retention.

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

No

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?

Access for internal parties is defined via the Staff Data Sheet (SDS). No external parties have access to system information. Internal contractors have FAR clauses to address privacy and ethics in Leidos, Inc, Contract Number: GS-35F-285DA.

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.

The System Security Plan defines retention for the purposes of system backups to be 3 years. The system information is retained in the form of backups, for the reason of restoring the system in the event of a technical failure. This is not an official record and does not require a Records Control Schedule 1012b. Records are maintained for 7 years.

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 retention of backups beyond the planned period may expose the data to a small risk of breach or tape corruption.

Mitigation:

The system uses least privilege access the system backups, limited to the System Administrators. Administrators maintain a schedule to purge backups kept beyond the retention period

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 information is shared externally.

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?

N/A

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. There is no external sharing

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 mechanisms to ensure the limited PII is accessed appropriately for the purpose of authentication, system access and least privilege are Active Directory (AD), ACLs, GPOs, Enterprise and local system policies and Agency-approved SCDs.

For the FieldOps analytic data, information use is governed by policy, the Rules of Behavior and CUI registry guidelines and enforced by the nature of the airgap network and least privilege.
Log and Event Manager (LEM) on both systems detects all administrative access to the data and notifications are sent to all system administrators.

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

The Information Security and Privacy Awareness Training is required annually and enhanced by the Cybersecurity Stand Down conducted annually.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Minimal chance of LEM failure to log anomalies and notify administrators in the event of misuse.

Mitigation:

Regular monitoring of LEM logs by System Administrator identifies possible gaps in notifications.

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.

Limited PII data is collected for authentication, system access, least privilege, creation and implementation of group policy, roles and auditing purposes(logs).

Analytic data is collected to establish environmental baselines, determine the extent, nature, and degree of harmful substances in support of radiation emergency response efforts. Analytic data is used to monitor, quantify, and identify radionuclides in support of radiation emergency response efforts.

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.*)

Administrative data is manually copied from Agency databases such as eBusiness or Active Directory. There is no retrieval of information on this system.
Analytic data is collected electronically by various radiation measurement instruments and systems. Instruments consist of handheld radiation monitors that output measurement data. Systems include computer-controlled radiation and various environmental monitors that allow continuous collection and analysis of data. There is no individual identifier associated.

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 identifiable information contained in the system is readily available business information from various Agency directories and does not impact personal privacy.

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:

Low risk of information misuse due to potential reporting.

Mitigation:

The system uses least privilege and need-to-know controls in accessing the storage of business identification data obtained from Agency-provided resources. Reporting of information logs and use can identify misuse.

***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: