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: National Enforcement Investigations Center Local Area Network (NEIC-LAN)	
Preparer: Michael Scales	**Office: OECA/OCEFT/NEIC**
Date: 10/26/2023	**Phone:** 303 462-9083
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 NEIC-LAN is a general support system that maintains Users Shares, Program Shares, and Minor Applications to support field staff, laboratory staff, legal staff, and facility and infrastructure supporting function staff.

The NEIC-LAN hosts the Master Tracking System (MTS). This is a minor application used to track employee support and contains project records related to scientific support for Civil, Criminal and Special projects performed at the NEIC laboratory.

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?

Authorities granted under Federal Environmental Laws and Regulation for Administrative/Civil Investigations

- Inspection Authority
    - Air - Clean Air Act (CAA, 42 U.S.C. § 7401) - 114, 206, 208, 504
    - Water - Clean Water Act (CWA, 33 U.S.C. § 1251) - 308, 402
    - Superfund – Comprehensive Environmental Response, Compensation, and Liability ACT (CERLA, 42 U.S.C. § 9601) – 103
    - Pesticides – Federal Insecticide, Fungicide and Rodenticide Act (FIFRA, 7 U.S.C. § 136) – 8, 9
    - Solid Waste – Resource Conservation and Recovery Act (RCRA, 42 U.S.C. § 6901) – 3007, 9005
    - Drinking Water -Safe Drinking Water Act (SDWA, 42 U.S.C. § 300f) – 1445
    - Toxics – Toxic Substances Control Act (TSCA, 15 U.S.C. § 2601) – 11
- Recordkeeping Authority
    - Air - Clean Air Act (CAA, , 42 U.S.C. § 7401) – 114, 208, 311
    - Water – Clean Water Act (CWA, 33 U.S.C. § 1251) – 308, 402
    - Superfund – Comprehensive Environmental Response, Compensation, and Liability ACT (CERLA, 42 U.S.C. § 9601) – 103
    - Pesticides – Federal Insecticide, Fungicide and Rodenticide Act (FIFRA, , 7 U.S.C. § 136) – 4, 8
    - Solid Waste – Resource Conservation and Recovery Act (RCRA, 42 U.S.C. § 6901) – 3001, 3002, 3003, 3004. 9003
    - Drinking Water -Safe Drinking Water Act (SDWA, 42 U.S.C. § 300f) – 1445
    - Toxics – Toxic Substances Control Act (TSCA, 15 U.S.C. § 2601) – 8
- Confidential information (40 Code of Federal Regulations [CFR] 2.201-2.215)
    - Air – Clean Air Act (CAA, 42 U.S.C. § 7401) - 208, 307, 40 CFR 2.301
    - Water - Clean Water Act (CWA, 33 U.S.C. § 1251) - 308, 40 CFR 2.302
    - Superfund – Comprehensive Environmental Response, Compensation, and Liability ACT (CERLA, 42 U.S.C. § 9601) – 104, 40 CFR 2.310
    - Pesticides – Federal Insecticide, Fungicide and Rodenticide Act (FIFRA, 7 U.S.C.

§ 136) – 7, 10, 40 CFR 2.307

- Solid Waste – Resource Conservation and Recovery Act (RCRA, 42 U.S.C. § 6901) – 3007, 9005, 40 CFR 2.305
- Drinking Water -Safe Drinking Water Act (SDWA, 42 U.S.C. § 300f) – 1445, 40 CFR 2.304
- Toxics – Toxic Substances Control Act (TSCA, 15 U.S.C. § 2601) – 14, 40 CFR 2.306

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, ATO expires 20 June 2020. Extension has been granted up until , Dec 31, 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).

Subjects of investigation about whom data has been collected by criminal investigators of the Office of Criminal Enforcement, Forensics and Training, Criminal Investigation Division, and assembled in the form of investigative reports concerning violations of federal environmental statutes and regulations.

The MTS collects project number, project name, employee name, employee telephone number, project status, case outcome, enforcement data such as planned dates of search warrants or facility inspections, types of analyses, employee testimony, witness interviews, regulatory histories, inspection notes, analytical results and other related investigative information.

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

There are two general categories of potential evidence.

- Samples and other physical evidence
- Records and documents

The MTS collects information from EPA Regional Offices, From OECA-OCEFT-CID special agents, direct from facility, thorough onsite inspection, through analytical analyses, employee input.

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 Data is reviewed on a quarterly basis to ensure accuracy.

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:

Risk of unauthorized printing or unauthorized sharing of information.

Mitigation:

Several layers including the agency network security process, NEIC roles which control access to these items, and the data entry process.

Records management procedures, including security clearances, training, and code of conduct. This includes PL-4 – Rules of Behaviors, CIO 2151.1 - Privacy Policy, and CIO 2150-P-21.0 – Information Security – National Rules of Behavior.

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, access is controlled by Active Directory Access Control Lists. Employees are assigned roles within the system and those roles control the access allowed. Project Managers have read write access, Principal Analytical Chemist have read write access, Responsible Management Officials have read write access, assigned team members have read write access, all others have only read access or no access.

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

User access is determined by role, access is granted by individual group or by access granted by the System Administrator. The following procedures contain sections that address the issue of access control.

NEICPROC/00-057 Security

NEICPLAN/01-002 NEIC LAN System Security Plan

NEICPROC/00-059 Evidence Management

NEICPROC /16-002 Configuration Management

NEICGUID/05-001 FOIA and Discovery/Litigation Requests for Information

NEICPROC/00-061 Records Management

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?

Only Federal employees of NEIC will have access to the data/information and it is controlled to an as needed basis. Contractors do not access the system.

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 EPA Records Control Schedule is 1044 – Compliance and Enforcement https://intranet.epa.gov/records/schedule/final/1044.html. Records are retained for 5,10, 20 years or permanently depending on enforcement outcome.

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 the risk that information will either be disposed before it has met the required retention or that it will be retained to long.

Mitigation:

Closed files are placed in the NEIC Records Center where they are monitored and controlled by trained records specialist. Records are recorded/retained in an agency approved record keeping system that helps control records retention and disposition.

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.

Yes, but not by NEIC. CID Offices or EPA Regions may share project information with the DOJ or possibly other partner federal agencies or state criminal investigative agencies.

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

The sharing of information from this system are compatible with the purposes of the collection. The NEIC MTS provides support in investigations of persons or organizations alleged to have violated any Federal environmental statute or regulation or, pursuant to a cooperative agreement with a state, local, or tribal authority, an environmental statute or regulation of such authority.

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 doesn't allow or grant direct access to data, through any of the means described, to anyone other than federal employees of NEIC, but the data may be shared by NEIC management with the folks described in 4.1, as appropriate for enforcement action.

4.4 Does the agreement place limitations on re-dissemination?

Yes

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:

There is a small risk that data will be shared inappropriately with organizations outside of EPA through direct access to the system.

Mitigation:

To minimize this risk, direct access to the data is only granted to federal employees of NEIC. Any sharing of data from the system is conducted and controlled by NEIC management review.

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)?

Agency network security process. Quarterly Reviews by NEIC Staff and Annual Continuous Monitoring Assessment Audit conducted by a Third Party. Records management procedures, including security clearances, training and code of conduct.

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 Annual Information Security and Privacy Awareness Training and the EPA Agency National Rules of Behavior training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk of improper auditing the auditor's inability to discover when data is inappropriately used or shared by system users

Mitigation:

To mitigate this risk we perform quarterly reviews of system access and use by NEIC staff and annual continuous monitoring assessment audit are conducted by a third party. Both the NEIC Quality Manager and team members and the NEIC Management team conduct assessment audits.

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.

To provide support in investigations of persons or organizations alleged to have violated any Federal environmental statute or regulation or, pursuant to a cooperative agreement with a state, local, or tribal authority, an environmental statute or regulation of such authority.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X__ 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.)

Paper information is stored in a Paper Project File Share and associated to a Project File Name. The Project File Name is how the information is retrieved, for criminal projects the **project file name may be an individual's name.** Employee name serves as the primary retrieval key for sections of the system.

Electronic information is stored in an electronic Project File Share and associated to a Project File Name. The Project File Name is how the information is retrieved.
Project File Name could be linked to an individual, business, site or specific case.

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

SORN in development for the MTS (EPA-79).

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 small risk that data is inappropriately used or shared by system users.

Mitigation:

To mitigate this risk, we provide mandatory annual training of all systems uses in Agency records management procedures, information security and privacy awareness. Continuous monitoring of information use and sharing. Information cannot be released outside NEIC without Management approval.

*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.

For criminal investigations individuals are not notified about the collection of information. This is a law enforcement system therefore there is no privacy risk as, pursuant to 5 U.S.C. 552a(j)(2), this system is exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and

(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in that subsection: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f)(2) through (5). See, 40 CFR 16.11 and 16.12. For civil investigations, individuals either do not receive, or do not sign the consent form during field investigations. For Civil investigations: During field investigations EPA Field personnel work directly with individuals and through a signed consent form. For Criminal investigations No prior notice is provided, because the data involves ongoing criminal investigations; or involves EPA discovery, receipt, or searches of open source online information, or other information or records outside the agency. In short, the records are exempt from Privacy Act notice. See, 40 CFR 16.11 and 16.12.

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?

For Civil cases individuals can decline to consent in which case information is only collected through a court order.

For Criminal cases **i**ndividuals do not have the opportunity to decline or provide information, or to opt out of the collection or sharing of their information

7.1 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:

Publishing the SORN without proper exemption.

Mitigation:

Exemptions are properly published.

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?

This is a law enforcement system, individuals are not allowed to access their information. Pursuant to 5 U.S.C. 552a(j)(2) this system is exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in that subsection: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f)(2) through (5).

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

This is a law enforcement systems, individuals are not provided the opportunity to correct or change information in anyway.

8.3 How does the system notify individuals about the procedures for correcting their information?

This is a law enforcement system, individuals are not provided the opportunity to correct 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:

Individuals may become aware of this system of records and want the opportunity to redress.

Mitigation:

The System of Records Notice for this system is published in the federal register with the exemptions to the privacy act.