United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – 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: Agency Labor and Employee Relations Tracking System (ALERTS)		**System Owner: Jeff Edwards OFA-OCIO-SIMD-EDB**	
Preparer: Jeff Edwards		**Office: OFA-OCIO-SIMD-EDB**	
Date: May 14, 2026		**Phone: 919-541-2677**	
Reason for Submittal: Update requested by Bobby Moore due to new template.			
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:

The EPA Labor and Employee Relations (LER) Division will use the Agency Labor and Employee Relations Tracking System (ALERTS) to track, manage, and report on a full spectrum of LER cases throughout the Agency. The system will validate user entry with respect to established business rules, present data to the

user for verification and update, and will allow authorized LER employees the ability to report data to their management, as directed. This system will enable LER employees to perform their duties effectively and proficiently.

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 USC Chapter 71

- 5 USC Chapter 43

- 5 USC Chapter 75

- CFR 771

- 5 CFR 752

- 5 CFR 432

- SORN: [EPA–HQ–OEI–2014–0466; FRL–10120–01– OMS]

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?

System Security Plan was completed and submitted on 12-20-2024. Approval received under EPA's M365 Application controls and operates under Email and Collaboration Solutions (ECS) ATO.
Expiration 10-31-2026

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.

Not applicable. The system is used by authorized EPA LER employees only (internal to EPA). No ICR 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?

The data will be stored in Microsoft's Government Community Cloud. The Power Apps GCC environment provides compliance with all FedRAMP High, DoD DISA IL2, and requirements for criminal justice systems.

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).

The ALERTS application will collect information about agency LER cases within three major areas:

- Labor Relations case file information collected for administrative grievances, grievances of the parties, negotiated grievances, formal discussions/meetings, union information requests, negotiations, unfair labor practices (ULP) charges, and unit clarification petitions.
- Employee Relations case file information regarding employee counselling for misconduct or poor performance, disciplinary actions, adverse actions, performance-based actions, performance assistance plans, performance improvement plans, general LER advisory services and Merit System Protection Board (MSPB) appeals.
- Information on investigation inquiries.

Data elements for all cases include employee names, organizational information, grades, bargaining unit status, union information, supervisory information, and case-specific data. For ease of reviewing this document, all data elements are listed at the end of this document. Please refer to those tables for a full list of data elements that will be in the ALERTS system.

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

The ALERTS system will have a connection to the OASIS data warehouse, which is a read-only data warehouse of HR related information that includes data from the Department of Interior (DOI) Federal Personnel Payroll System (FPPS). The ALERTS application will receive the following data elements from OASIS:

- Position Title
- Pay Plan
- Pay Grade
- Series
- Entrance on Duty to the Agency
- Leave Service Computation Date
- Bargaining Unit Code
- Duty Location

Authorized LER users input case-specific information generated from each individual case.

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, the system will not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

If a user identifies that data coming from OASIS is incorrect, they will follow established Agency procedure to update the incorrect data in the DOI FPPS system. For data that is entered into and managed by agency users, the accuracy of the data will be ensured by regular reviews conducted by authorized users in the HQ LER Division. These reviews will be conducted by designated HQ LER staff, depending on the type of file/case. If there are discrepancies, the HQ LER reaches out to the region/LER specialist who entered the case, and they work to resolve the discrepancy. In addition, the system will implement business rules where applicable to ensure data quality. Examples include reference data lists for some selections, rules that implement logic for one field based on the selection of other fields, enforcing data type rules (i.e., dates must be dates, etc.)

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 main privacy risk in the ALERTS application is that case information will be viewable by EPA employees other than authorized users.

Mitigation:

The ALERTS application mitigates this risk by controlling user read/write access to the application using implemented controls within Dataverse that are maintained by Microsoft and covered under the platformlevel ATO. Only authorized users in EPA's LER user community will be able to view data within the system. Authorized users will be determined by EPA HQ LER who have the personal knowledge of the individual's need to access information in the system. There is also a privacy/warning notice that is displayed to all users upon login/entering the system.

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, Microsoft365 has access roles assigned to users through an administrative group. Access to the ALERTS application will occur through MS365 which requires agency users to sign on using their PIV card, computer password and, if working remotely, additional access through a VPN.

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

Microsoft maintains the documentation for column level security, here: https://learn.microsoft.com/en-us/power-platform/admin/field-level-security.

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

No. There are no other components with assigned roles or 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?

Access and use of the system is limited to a select group of a small number of agency LER specialists, legal staff, and system support staff who have a need to know this information. Access is granted only through approval by the Division Director of LER. Once that approval is received, only then can the user be added to the appropriate security group. Contractors will not have access to this 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.

Information is maintained 50 years after filing closure or when the data is no longer needed for Agency business. This data is covered by EPA Records Schedule 0756.

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 data for this application will be retained in Dataverse for a longer length of time than necessary, if EPA determines that the timeframe for “no longer needed for Agency business” is a short period of time.

Mitigation:

Dataverse is a Platform-Level capability/controls maintained by Microsoft and already covered under the platform-level ATO.

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 governments, 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.

Data is not provided outside of EPA as part of normal agency operations. The ALERTS system is for internal EPA use only.

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

Not applicable; see 4.1.

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?

Not applicable; see 4.1.

4.4 Does the agreement place limitations on re-dissemination?

Not applicable; see 4.1.

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:

Not applicable; see 4.1.

Mitigation:

Not applicable; see 4.1.

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?

Only EPA Government personnel have access to the system. ALERTS utilizes access level controls to ensure that only the appropriate users, in the appropriate security roles, are exposed to the appropriate level of information. Application owners will ensure that these users are properly trained on the use of this system and its associated data.

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

There is a privacy statement associated with this data. Additionally, mandatory EPA Information Security and Privacy Awareness Training is required for all employees on an annual basis.

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:

Lack of auditing could risk exposing data.

Mitigation:

EPA reviews system level access controls and give access to authorized LER users only or employees deemed to be need-to-known.

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.

The ALERTS application will be used to store case files for all LER activities to include unfair labor practices, negotiation information, union notice, grievance files, performance actions, misconduct actions, informal advisory services, etc. The system is used as a record-keeping system as a means for the agency to ensure consistency with regard to agency LER actions.

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.

In order to retrieve information, users pull information primarily by employee name, employee email, or case type and date.

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.

Access to this system is limited to only users who have been added to the appropriate security group for the Microsoft Power Platform application. Access to that security group is limited to the LER Division Director. Users will only include authorized EPA LER employees or other EPA employees (i.e., labor attorneys) deemed to require access on a need-to-know basis, as determined by the LER Division Director. Access will be limited to employees who need to know the information in order to perform their official duties.

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 information collected and maintained in the system could be misused by authorized users.

Mitigation:

The system is designed and limited for use by a limited group of individuals who deal with information related to employee disciplinary files daily. The LER community is employed to assist managers and the agency with confidential performance and conduct matters; therefore, this community is acutely aware of the risk of releasing confidential disciplinary records. Access to the system, including its reporting functionality, is exclusively limited to this community.

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?

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.

7.3 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:

None, as the ALERTS system will not provide individuals with notice as ALERTS has no effect on the privacy of individuals. The system keeps records consistent with the federal registrar notice and the system keeps records of the management deliberative process related to performance/misconduct actions.

Mitigation:

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:

None. There are appropriate procedures in place to address all requests related to redress.

Mitigation:

None. Publication of information on PAR procedure on the EPA's public-facing website.

I attest as the Agency Privacy Officer that **Agency Labor and Employee Relations Tracking System (ALERTS)** 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,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.09.04 14:48:57 -04'00'

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