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: Agency Labor and Employee Relations Tracking System (ALERTS)	
Preparer: Jeff Edwards	**Office: OMS/OHCO**
Date: 2024-10-20	**Phone: 919-541-2677**
Reason for Submittal: New PIA__X__ Revised PIA____ 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:

Agency Labor and Employee Relations Tracking System (ALERTS) is being developed in Microsoft Power Platform to replace the decommissioned Labor and Employee Relations Tracking System (LERTS). EPA Labor and Employee Relations (LER) Division will use 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.

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?

- 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?

The ALERTS application is utilizing a system (M365 Power Platform) at EPA operating with an ATO under the Email and Collaboration Solutions (ECS) ATO which expires on November 10, 2025.

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 2.0 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 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 investigative inquiries relating to EPA's anti-harassment program under EPA Order 4711.

Data elements collected in all three categories of cases above include employee names, organizational information, grade, bargaining unit status, union information, supervisory information, and case-specific data. Case specific information could also include medical information, financial information, address, date of birth, and/or social security number. Please refer to detailed tables in the PTA for a full list of data elements to be processed by 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 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:

Given the sensitivity of the information, there is a risk of compromise of case information should unauthorized users view the information, some of which pertains to criminal conduct and has serous privacy implications for individuals and the agency.

Mitigation:

The ALERTS application mitigates privacy risk by deploying privacy and security controls from the current NIST 800-53. User read/write access to the application is controlled using implemented controls within Dataverse that are maintained by Microsoft and covered under the platform-level 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 3.0 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, 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?

ALERTS access controls align with EPA's Access Control Procedures. Microsoft also 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 file closure or when the data is no longer needed for Agency business. This data is covered by EPA Records Retention 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:

There is a risk that the data for this application will be retained in Dataverse longer than authorized.

Mitigation:

Periodic reviews of retention schedules are conducted to ensure information is not retained longer than authorized.

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.

Data is not shared externally as part of normal EPA 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 5.0 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?

- 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.
- Reviews of and updates to this PIA every three years or as needed with NPP approval.
- The system will undergo annual third-party security assessments for continuous monitoring and in support of the system's Authority to Operate (ATO).
- Ensuring that users receive mandatory security and privacy training annually.

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

Mandatory EPA Information Security and Privacy Awareness Training is required for all employees on an annual basis. There is also a Privacy Act Statement associated with this data.

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:
There is a risk that lack of auditing could lead to a compromise.

Mitigation:
EPA implements key controls including annual Information Security and Privacy Awareness Training for all users, PIA reviews and system security assessments, system user access controls, application audit logs detailing user activity and continuous monitoring.

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 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 regarding agency LER actions.

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.*)

Users retrieve 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.]

To evaluate probable or potential impacts on privacy of individuals, EPA conducts periodic Privacy Threshold Analyses, Privacy Impact Assessments and privacy risk assessments associated with the SORN for the records processed by the system.

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 has role-based access control (RBAC) in place and the system is designed and limited for use by a limited group of individuals who deal with information related to employee disciplinary files daily. EPA also uses auditing logs to enhance the supervision checks and audit trails to report all access and operation of the system. Periodic assessments, continuous monitoring and OIG oversight also ensure PII is used as authorized.

*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.

Users view a Privacy Act Statement at logon. The system is covered by a SORN that is publicly accessible.

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?

Individuals with LER case cannot decline to provide information. Some of the data in ALERTS is pulled from OASIS. See section 2.2 above.

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:

There is risk of inadequate notice to individuals.

Mitigation:

Publication of the SORN associated with the system and Privacy Act Statement at log on. The system processes and stores records (including management deliberative process related to performance/misconduct actions) consistent with the SORN. If an employee is disciplined, the official record of this disciplinary action is maintained in their electronic Official Personnel File to which the employee has access.

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?

The EPA operates a Privacy Act Request procedure. 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?

The Privacy Act Request procedure. 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 FOIA.

Privacy Risk:

Individuals' lack of awareness of Privacy Act Request procedure.

Mitigation:

Publication of information on PAR procedure on the EPA's public-facing website.