



# 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](https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx)

<b>System Name: Labor and Employee Relations Information System (LERIS)</b>	
<b>Preparer: Renee Gutshall</b>	<b>Office: OMS/OHR/LER</b>
<b>Dan Goddard (CTR)</b>	<b>Office of Mission Support (OMS)</b>
<b>Date: May 27, 2021</b>	<b>Phone: 202-566-0987</b>
<b>Reason for Submittal: New PIA</b> <input type="checkbox"/> <b>Revised PIA</b> <input type="checkbox"/> <b>Annual Review</b> <input checked="" type="checkbox"/> <b>Rescindment</b> <input type="checkbox"/>	
<b>This system is in the following life cycle stage(s):</b>	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
<b>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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u></b>	
<b>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u><a href="#">OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</a></u></b>	

## **Provide a general description/overview and purpose of the system:**

The Labor and Employee Relations Information System, also known as LERIS, is a Contractor system. LERIS is a Software as a Service (SaaS) offered by GDC Integration, Inc. (GDCI). This system offers Labor and Employee Relations (LER) specialists the capabilities to track, manage and report on a spectrum of labor and employee relations cases. The system validates entries in respect to the business rules, presents it for user verification and update, and allows information to be reported to upper management. It is a resource for federal LER specialists to effectively and proficiently address their job duties within proscribed legal parameters.

## **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; 5 CFR 771; 5 CFR 752; 5 CFR 432

### **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, the SSP has been completed. The system ATO expires on October 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?**

Yes, the data will be maintained or stored in a cloud. The CSP, GDC Integration, Inc. - General Support System (GSS), received FedRAMP authorization on May 10, 2021. For LERIS, the CSP provides SaaS.

## **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 collects information about agency LER cases within three major areas. Labor relations case file information is collected for administrative grievances, grievances of the parties, negotiated grievances, formal discussions/meetings, union information requests, negotiations, unfair labor practice (ULP) charges, and unit clarification petitions. Employee relations case file information is collected for employee counseling 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. The third area collects information on EPA's anti-harassment program under EPA Order 4711, including allegations, fact-finding reports and results. Data elements for all cases include employee name, organizational information, grade, bargaining unit status, union information, supervisory information and case-specific data.

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

The Department of Interior (DOI) Federal Personnel Payroll System (FPPS) provides LERIS with general human resources elements, to include First/Middle/Last Name, Appointment Type, Appointment Not-to-Exceed Date (if applicable), Service Computation Date for Leave Accrual Purposes, Service Computation Date for Retirement Eligibility Purposes, Position Title, Pay Plan, Occupational Series, Grade, Step, Supervisory Code, Bargaining Unit Status Code, Organizational Breakdown of Position's Location ("Organization Level 1" through "Organization Level 8," as applicable) and Duty Station. LER specialists' input relevant information for each individual case including supporting documents.

## **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. Data for the system is from the Federal Personnel and Payroll System (FPPS).

## **2.4 Discuss how accuracy of the data is ensured.**

When a LER specialist creates a new case, data is populated from the Federal Personnel and Payroll System (FPPS) into locked fields. These fields cannot be modified. If data is noted to be incorrect, the LER Specialist will need to contact the Shared Service Center.

## **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 privacy risks related to the characterization of the information include risks of exposing confidential employee disciplinary information and confidential labor relations strategies.

### **Mitigation:**

This risk is mitigated by the following controls:

- Access to the system is limited to 55 EPA labor and employee relations staff and employment law attorneys with a need-to-know for the information.
- Accounts are assigned from EPA Headquarters LER, who have personal knowledge of each individual's need to access the information in the system.
- There is a privacy/warning notice that is displayed on each login.
- Each user must log in with a username and password each time they access the system.
- Users must log in every thirty (30) days or they are blocked out of the system and they must contact the EPA LERIS administrator to be re-authorized for access.
- Users are logged off after 18 minutes of inactivity.

## **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?**

LERIS has layered access control levels with the systems.

1. User – this is the basic access provided to all users.
2. Administrator – this is limited to the System Administrators who have access to the system in both the production and in the test environment.
3. Sensitive Case Access – this access is limited to a handful of LER staff and managers. Sensitive cases include cases that may be underway regarding political employees, SES or other high-level employees.

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

The LERIS Access Controls are documented in the System Security Plan (SSP) and the LERIS Account Management SOP.

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

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 maximum of 55 agency Labor and Employee Relations (LER) specialists and legal staff who have a need to know this information. Access is granted only through approval by the Division Director of LERD. The Privacy Act FAR clauses are in the pending contract.

**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 destroyed 50 years after file closure or when the data is no longer needed for Agency business in accordance with RCS 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:**

Per Records Control Schedule 0756, records are destroyed 50 years after file closure or when the data is no longer needed for Agency business. This is long time to maintain the records based on the sensitivity of the information they contain. There is a risk that a large volume of sensitive data could be unintentionally accessed and compromised.

**Mitigation:**

This risk is mitigated by limiting access to the LERIS system to only those with a very clear need-to-know. LERIS employs role-based access control to limit the access to a small, defined group of EPA personnel. In addition, LERIS can only be accessed from the EPA network preventing access from external parties.

## **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.**

LERIS is for internal EPA use only with no information sharing or external reporting.

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

No external sharing.

**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?**

None.

**4.4 Does the agreement place limitations on re-dissemination?**

No agreement.

**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 outside of EPA.

**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?**

Only EPA Government personnel have access to the system. LERIS utilizes account management and auditing to ensure that the information is used as stated in Section 6.1. EPA LERIS Administrators have access to audit information that includes a history of who created, modified, closed, canceled, or reopened a case and the date and time associated with it.

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

The agency conducts mandatory annual IT Security and Privacy Awareness training. This training includes a user signature attesting that they will abide by privacy-related requirements in applicable EPA Rules of Behavior documents and that they may be subject to disciplinary action if they knowingly violate these privacy-related requirements. In addition, LER specialists must agree with these Rules of Behavior every time they sign into the system.

## **5.3 Privacy Impact Analysis: Related to Auditing and Accountability**

### **Privacy Risk:**

Improper or infrequent audit log reviews may not detect the misuse of information.

There is a risk that personnel do not complete annual Privacy Training.

### **Mitigation:**

The audit logs are reviewed in accordance with the EPA CIO AU procedure.

With respect to Privacy Training, this risk is mitigated by keeping suitable record and disabling access to personnel who do not complete the mandatory annual training.

## **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 information is needed to provide the foundational information on each case in LERIS. The information is used by LER specialists to make informed decisions about the direction of a case.

### **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.)**

The system is designed to retrieve information by employee name, case number, case type, or date. The only personal identifier used to retrieve information is the employee name.  
EPA-68

### **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 system administrator and LER Division Director evaluate the individuals with access to the system on a regular basis. LERIS users are limited to LER specialists and agency attorneys who have a need to know.

### **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 unauthorized users may access records in EPA LERIS.

There is a risk that information collected and maintained in LERIS could be misused by authorized users.

#### **Mitigation:**

Access to the EPA LERIS instance is limited to authenticated and registered EPA users. These users are authenticated at each connection attempt before access is granted. In addition, the risk that unauthorized users could access LERIS information in transit is mitigated by encrypting all communication flows between EPA and LERIS.

Authorized users are assigned to one of the three roles within the EPA LERIS instance based on their need to use the information. Prior to granting access to the system, EPA LERIS displays a warning banner on the login screen to advise all users about proper and improper use of the data, that the system may be monitored to detect improper use, and the consequences of such use of the data. Users must acknowledge that they have read and will abide by the instructions in the warning banner.

**\*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.**

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](mailto: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](mailto: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. The system does not provide individuals with notice as LERIS has no effect on the privacy of individuals. The system keeps records consistent with the federal registrar notice. The system keeps records of the management deliberative process related to performance/misconduct actions.

#### **Mitigation:**

None. If an employee is disciplined, the official record of this discipline is maintained in his/her electronic Official Personnel File, to which the employee has access. Official negotiation/labor relations files are not related to individual employee privacy information, therefore no notice is required.

## 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?**

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.

As discussed in Question 2.2, data is imported from FPPS. If there are issues with an employee's basic data then personnel should follow procedures documented in the publicly-available Department of Interior (DOI) FPPS PIA.

### **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 FOIA.*

#### **Privacy Risk:**

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

#### **Mitigation:**

None.