U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Employee and Labor Relations Tracking System (ELRTS)

Bureau/Office: Office of the Chief Information Officer
Date: March 15, 2019
Point of Contact:
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: 202-208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC, 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Department of the Interior (DOI), Office of Human Capital (OHC), manages the Employee and Labor Relations Tracking System (ELRTS). ELRTS is a department-wide system used by Human Resources (HR) employee and labor relations staff and Servicing Personnel Offices (SPOs) to track a broad scope of HR activities that require action. ELRTS will help HR

personnel create, read, update, and manage employee and labor relations cases, including administrative grievances, adverse actions, disciplinary actions, medical leave requests, performance improvement plans, performance based actions, reasonable accommodation requests, arbitration requests, impasses, negotiated grievances, negotiations / duty to bargain notices, negotiability disputes, representation / organizing proceedings, and unfair labor practices. ELRTS provides functionality and processing capability required to collect, track, manage, process, and report on information regarding business processes, and analyzes trends. It allows HR staff to track the status and stage of employee and labor relations cases and helps DOI comply with statutory, regulatory, and executive reporting requirements.

The DOI OHC oversees management of ELRTS at the department level, however, cases are created, tracked and resolved by bureau and office SPOs. All DOI bureaus and offices are required to use ELRTS as prescribed to record case file information for all covered cases in accordance with documented guidelines, with the exception of the Office of Inspector General (OIG).

ELRTS is a customization of the Salesforce platform hosted in the Salesforce Government Cloud that is FedRAMP authorized. The Salesforce Government Cloud is a partitioned instance on the platform as a service (PaaS) and software as a service (SaaS). It is a multi-tenant community cloud infrastructure specifically for use by U.S. federal, state, and local government customers, U.S. government contractors, and federally funded research and development centers.

C. What is the legal authority?

5 U.S.C. Chapter 43 - Performance Appraisal; 5 U.S.C. Chapter 71 - Labor Management Relations; 5 U.S.C. Chapter 75 - Adverse Actions; 5 U.S.C. Section 2301; 5 CFR Part 293 - Personnel Records; 5 CFR Part 351 - Reduction in Force; 5 CFR Part 430 - Performance Management; 5 CFR Part 432 - Performance Based Reduction In Grade And Removal Actions; 5 CFR Part 531 - Pay under the General Schedule; 5 CFR Part 752 - Adverse Actions; 5 CFR Part 771 - Agency Administrative Grievance System; 5 CFR Part 1201 - Practices And Procedures; 5 CFR Part 2422 - Representation Proceedings; 5 CFR Part 2423 - Unfair Labor Practice Proceedings; 5 CFR Part 2424 - Negotiability Proceedings; Executive Order 13839: Executive Order on Promoting Accountability and Streamlining Removal Procedures Consistent with Merit Systems Principles, dated May 25, 2018; 370 DM 771 - Administrative Grievance Procedures; 370 DM 752 - Discipline and Adverse Actions; 370 DM 430 - Performance Management System.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems

☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000000309 00-00-01-07-02-00; Employee and Labor Relations Tracking System-Salesforce SSP

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

This system manages and tracks cases for HR oversight and action and is not intended to replace or maintain the official case records maintained under government-wide and department-wide systems of records notices depending on the type of case being tracked. These notices may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

- DOI-74: Grievance Records, 64 FR 19381 (April 20, 1999)
- DOI-77: Unfair Labor Practice Charges/Complaints Files, 64 FR 18434 (April 14, 1999)
- DOI-78: Negotiated Grievance Procedure Files, 64 FR 19383 (April 20, 1999)
- OPM/GOVT-1: General Personnel Records, 80 FR 74815 (December 11, 2012)
- OPM/GOVT-2: Employee Performance File, 71 FR 35347 (June 19, 2006)
- OPM/GOVT-3: Records of Adverse Actions, Performance Based Reductions in Grade and Removal Actions, and Terminations of Probationers, 71 FR 35350 (June 19, 2006)
- MSPB/GOVT-1: Appeals and Case Records, 67 FR 70254 (November 21, 2002)

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name	☐ Religious Preference	☐ Social Security Number (SSN)
☐ Citizenship	☐ Security Clearance	☐ Personal Cell Telephone Number
☐ Gender	☐ Spouse Information	☐ Tribal or Other ID Number
☐ Birth Date	☐ Financial Information	☐ Personal Email Address
☐ Group Affiliation	☒ Medical Information	☐ Mother's Maiden Name
☐ Marital Status	☒ Disability Information	☐ Home Telephone Number
☐ Biometrics	☐ Credit Card Number	☐ Child or Dependent Information
☐ Other Names Used	☒ Law Enforcement	☒ Employment Information
☐ Truncated SSN	☐ Education Information	☐ Military Status/Service
☐ Legal Status	☐ Emergency Contact	☐ Mailing/Home Address
☐ Place of Birth	☐ Driver's License	☐ Race/Ethnicity

☒ Other: *Specify the PII collected.*

Information is maintained on former or current DOI employees who made requests to HR or filed formal grievances and complaints on labor relations, conduct and/or performance issues. PII includes employment related data such as employee common identifier, organization, position title, pay plan, series, grade, duty station, email, phone number, and information related to a grievance, complaint, or request. Other PII data may include transcripts of hearings; and relevant information about other individuals in complainants' work units, statements of witnesses, reports of interviews, examiners' findings and recommendations, correspondence and exhibits, however official copies of original and final decisions on the grievances / complaints filed are not stored in ELRTS. Some types of misconduct may be criminal in nature or complaints may allege criminal activity that may involve law enforcement investigations or records. Employee requests for reasonable accommodation or medical leave may include information related to medical, disability, or type of accommodation requested and provided by the agency.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency

☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

Information is entered into ELRTS by an HR specialist in response to an inquiry, complaint or grievance brought by a DOI employee, supervisor or legal representative with knowledge of the allegation or case. The HR specialist working on a case may also obtain information from open sources, such as internet search engines, for investigative purposes. Information such as medical or disability forms, when provided, may be scanned and uploaded into ELRTS as supportive documentation.

Active Directory Federation Services (ADFS) will be used to access the system through single-sign-on. Information will be loaded from DOI Records into ELRTS such as name, position title, series, grade, duty station, etc. Information may also be migrated from other supporting systems into ELRTS.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Web site
☐ Fax
☒ Telephone Interview
☒ Information Shared Between Systems *Describe*
☐ Other: *Describe*

Information pertaining to employee and labor relations cases that arise in DOI come to the attention of designated and authorized HR staff through face-to-face, telephone, and/or email contact with employees and/or supervisors who have a employee or labor relations inquiry or issue. Evidentiary documents, materials, and comments may also be received in paper format and uploaded as an attachment. Relevant information is collected in this manner by the HR specialist, and is manually entered into ELRTS for case tracking by the HR specialist.

D. What is the intended use of the PII collected?

Employee PII is required for verification, identification and tracking purposes for department-wide computerized record keeping of labor and employee relations cases including:

- Administrative Grievances
- Adverse Actions
- Disciplinary Actions
- Medical Leave Requests
- Performance Improvement Plans

- Performance Based Actions
- Reasonable Accommodation Requests
- Arbitration Requests
- Impasses
- Negotiated Grievances
- Negotiations / Duty to Bargain Notices
- Negotiability Disputes
- Representation / Organizing Proceedings
- Unfair Labor Practices

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Within each bureau or office, information contained in ELRTS would be shared only with officials who have a need-to-know employment-related case information.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

The following bureaus or offices are users of the ELRTS application and would have access to data for other bureaus or offices due to cross-servicing relationships or other official functions.

- Office of the Secretary (OS), Office of Human Capital (OHC) – access to department-wide data for HR purposes.
- Office of the Secretary (OS), Interior Business Center (IBC) – access to OS organization data for HR purposes.
- Bureau of Safety and Environmental Enforcement (BSEE) – access to BOEM and OS organization data for HR purposes.
- U.S Geological Survey (USGS) – access to SOL data for HR purposes.
- U.S. Fish and Wildlife (FWS) – access to BLM Alaska data for HR purposes.
- Bureau of Land Management (BLM) – access to NPS National Interagency Fire Center (NIFC) data for HR purposes.
- Office of Inspector General (OIG) – OIG is not a user of the system, but may be provided data, including PII, in the performance of their official functions when necessary and authorized.
- Freedom of Information Act / Public Affairs (FOIA/PA) Offices – FOIA/PA is not a user of the system, but may be provided data, including PII, when necessary and authorized by law.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Other federal agencies do not have direct access to ELRTS. DOI may share records with OPM, the Merit Systems Protection Board, or the Federal Labor Relations Authority to perform their

authorized functions, other federal agencies or organizations to support investigations, settle complaint or appeals, or as authorized under the Privacy Act and the published routine uses contained in the applicable system of records notice. See OPM/GOVT-1: General Personnel Records, OPM/GOVT-2: Employee Performance File, OPM/GOVT-3: Records of Adverse Actions, Performance Based Reductions in Grade and Removal Actions, and Terminations of Probationers, MSPB/GOVT-1: Appeals and Case Records, DOI-74: Grievance Records, DOI-77: Unfair Labor Practice Charges/Complaints Files, and DOI-78: Negotiated Grievance Procedures Files, system of records notices which may be viewed at https://www.doi.gov/privacy/sorn

Aggregated reports with HR performance metrics, such as number of cases, types of cases, or results of cases, may be shared with OPM or other federal agencies; however, these reports do not contain specific PII on individuals.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Data is not routinely shared with tribal, state or local agencies. However, DOI may share records as authorized, consistent with the routine uses in the applicable published system of records notice as permitted by the Privacy Act.

☒ Contractor: *Describe the contractor and how the data will be used.*

Contractors are responsible for the operations and maintenance of the software platform. Salesforce support personnel need access to the platform to provide support and maintenance for the application that hosts PII, but will not have access to the database and the actual PII data. This maintenance is critical to protecting the system and the PII contained within the system. Salesforce maintains a FedRAMP authorization and undergoes a security assessment by a third party assessment organization (3PAO) each year.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

For instances where a complaint is filed on behalf of an individual or the individual has received legal representation, written consent must be obtained from the individual before sharing information with the authorized third party.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Employees voluntarily provide PII when they complete the Administrative Grievance Form AGF (DI-7600) or contact DOI HR staff to file a complaint or make a request for HR action. Employees are not compelled to provide any PII information, however failure to provide

sufficient information may impair DOI HR staff ability to review allegations, respond to requests for reasonable accommodation or other requests. Employees may file complaints anonymously, however, it may be difficult for HR to investigate allegations without identifying information of the employee who is making the allegation. Every DOI employee may request that their information be kept confidential, and DOI HR staff will honor those requests to the extent to which confidentiality can be provided under applicable laws and regulations.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is provided when collecting PII directly from employees.

☒ Privacy Notice: *Describe each applicable format.*

A privacy notice is provided to employees or supervisors by HR staff at the time a request is made and an employee or labor relations case is created, as well as in subsequent follow-up communication requiring PII.

Notice is provided on the Administrative Grievance Form AGF (DI-7600).

Notice is also provided to DOI employees through the publication of this PIA and the applicable published SORNs that cover the records tracked by this system.

☒ Other: *Describe each applicable format.*

HR personnel are provided with a privacy and security warning banner when accessing the system.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data is generally retrieved manually by authorized and authenticated users, but can also be retrieved via reports generated by system. Identifiers that can be used to retrieve the data include the name of individual, employee common identifier, or case number.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Reports can be produced on individuals who are the subject of an employee relations or labor relations case. Such reports will be used to inform authorized users and officials with a need-to-know on the status and/or disposition of a particular case. Data included in such reports will vary but can include name, organization, address, telephone, date of events related to the case, subject of the case, case events, supervisor, disposition of the case, etc.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Information gathered is from DOI employees, supervisors and/or subordinates, and will be verified via established investigative procedures such as investigating allegations and statements and comparing statements and facts in order to determine the truth. Official findings and conclusions derived from these investigations are not stored in ELRTS. Employees and their representatives are given copies or access to information directly related to issues raised in the case upon request, unless doing so would be unduly burdensome or contrary to law or regulation as determined by the Servicing Personnel Office.

B. How will data be checked for completeness?

Information gathered will be verified based on established laws and regulations, and procedures based on employee reply and response processes to proposed personnel actions as established by law and policy. Identity of involved subjects is confirmed through in-person interviews and Personal Identity Verification (PIV) cards.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Cases will be actively managed in the system until a case is closed out, ensuring that the data is current through established investigative and HR procedures. Case status can be updated and/or closed by the HR specialist as appropriate.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Records retention depends on the type of case, the approved records retention schedule and the needs of the agency. ELRTS records are generally maintained under Departmental Records Schedule (DRS) 1.2A.0004, Short-term Human Resources Records, and 1.2B.0005, Long-term Human Resource Records, which were approved by the National Archives and Records

Administration (NARA) DAA-0048-2013-0001. These records include agency personnel records relating to requests for reasonable accommodations and the supervision and management of federal employees (labor management relations and arbitration files) when held by the negotiating office, and require additional retention generally to conform to preservation standards in specific regulations, policies, or other legal/statutory requirements. The disposition of these records is temporary. Records will be cut-off at the end of the fiscal year in which the case is closed or as specified in agency/bureau records manual, and destroyed 3 or 7 years after cut-off.

Records may be subject to litigation holds, which will override any records retention schedule or DOI policy that cover the transfer, disposal, or destruction of relevant records until the hold has been removed by an authorized authority.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and the 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a privacy risk related to hosting, processing and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information from ELRTS. These risks are mitigated through a combination of physical, administrative, and technical controls.

There is a risk that individuals may not know why their information is being collected, how it will be used or who it will be shared with during the course of investigations or HR actions to respond to employee requests or complaints. Employees are provided a Privacy Act statement upon request when providing information to HR officials. PII is necessary to facilitate the efficient review and resolution of HR matters and to provide a factual basis for the improvement of DOI policy. Employees are provided with DOI policies and procedures regarding employee and labor relations or other HR matters through departmental policy: 370 DM 771- Administrative Grievance Procedures, 370 DM 752 - Discipline and Adverse Actions and 370 DM 430 - Performance Management System. Employees are also provided notice of the collection, uses and sharing of information through the publication of this PIA and the applicable system of records notices: OPM/GOVT-1: General Personnel Records; OPM/GOVT-2: Employee Performance File; OPM/GOVT-3: Records of Adverse Actions, Performance Based Reductions in Grade and Removal Actions, and Terminations of Probationers; MSPB/GOVT-1: Appeals and Case Records; DOI-74 Grievance Records; DOI-77 Unfair Labor Practice Charges/Complaints Files; and DOI-78 Negotiated Grievance Procedures Files.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk access to data is restricted to authorized HR personnel with a need-to-know basis to preserve the integrity of data in the information system. The system and documents pertaining to investigations in ELRTS are closely safeguarded in accordance with applicable laws, rules and policies. Access to files is strictly limited to authorized personnel in writing who require access to perform their official duties and specified as to the level of access within each bureau or office. Access to administrative functions is strictly controlled and can only be granted by the ELRTS system administrators. System administrators periodically review audit logs to prevent any unauthorized monitoring. Users are also required to sign rules of behavior. All users must have a DOI account and government issued personal identity verification (PIV) card to access ELRTS. System administrators utilize operational and technical controls such as user identification, passwords, firewalls, encryption, audit logs, least privileges, malware identification, periodic verification of system users, and data loss prevention policies also help limit these risks and ensure appropriate permissions and access levels are enforced.

There is a risk that PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. This risk is mitigated by ensuring that data gathered in the system is protected from unauthorized disclosure and maintained in the investigative file. The system utilizes audit logs to monitor users' access and actions in the system to protect against any unauthorized access, changes or use of data. System users, by definition, occupy positions that require them to be well-prepared for handling sensitive issues. Designated HR users of the system are required to take annual mandated security, privacy and records management as well as role-based training where applicable training and sign the DOI Rules of Behavior prior to accessing the system. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is also risk that erroneous information may be collected. This risk is mitigated by allowing grievants to request access or amendment of their records at any time. Employees filing grievances are given access to their records as part of the official grievance process. Employees, may at a later date access their information by submitting a written request to the appropriate System Manager. Requests from individuals seeking amendment of their records which have been the subject of a judicial or quasi-judicial action will be limited in scope. Review of these requests will be restricted to determining if the record accurately documents the action of the agency ruling on the case and will not include a review of the merits of the action, determination, or finding.

There is also a risk that information in the system will be maintained longer than necessary to achieve the agency's mission. This risk is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. The data collected and stored is limited to the amount of data needed to track and manage employee and labor relations cases. Users are also reminded through policy and training that they must follow the applicable retentions schedules and requirements of the Federal Records Act.

There may be a risk associated with hosting the system with a cloud service provider. ELRTS is hosted in the Salesforce Government Cloud that is FedRAMP authorized. The Salesforce Government Cloud is a partitioned instance on the platform as a service (PaaS) and software as a service (SaaS). It is a multi-tenant community cloud infrastructure specifically for use by U.S. federal, state, and local government customers, U.S. government contractors, and federally funded research and development centers. $Salesforce maintains FedRAMP authorization and undergoes a security assessment by a third party assessment organization (3PAO) each year.$

Salesforce support personnel require access to the platform to provide support and maintenance for the application that hosts PII, but will not have access to the database and the actual PII data. This maintenance is critical to protecting the system and the PII contained within the system. ELRTS has undergone a formal Assessment and Authorization for issuance of an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and has been rated as a moderate system that requires management, operational, and technical controls in accordance with the NIST SP 800-53 as mandated under the FedRAMP authorization process. As part of the continuous monitoring program, continual auditing will occur on the system to identify and respond to potential impacts to PII information stored within the ELRTS environment.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The system allows the organization to manage employee and labor relations cases, which occur in the course of business for all bureaus or cffices. The use of PII data helps employee and labor relations staff to accurately identify and investigate allegations and statements of DOI employees and respond to employee requests.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

N/A. No new data is created by the system.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe*

Only authorized users, authenticated using a DOI PIV card and PIN, can access the system. Only authorized HR personnel and DOI system administrators will have access to data in the system. System administrators are authorized DOI HR personnel, and have access for user account management purposes and technical support. Contractors and developers will not have access to the production environment, therefore they will not have access to PII data in the system.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

User access is restricted by organization (bureau or office) and need-to-know through authorized job functions. Each bureau or office Human Resources Director authorizes employee access to

ELRTS in writing based on their official duties and responsibilities. A record of employees with access to ELRTS is maintained by each bureau or office employee and labor relations officer. Access is controlled through user account management and authentication with the DOI Active Directory system. Only authorized DOI personnel will have access to the system, and that access is based on the least privilege necessary to perform job duties.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy Act clauses are included in the ELRTS service contract.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The system does not locate or monitor individual employees who are subjects of cases. However, the system does identify and monitor user activities within the system through audit logs.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

ELRTS is not intended to monitor employees who are subjects of cases, however system administrators can use audit logs to identify any unauthorized monitoring of individuals. Through the auditing process username, IP address, time/date and login status, and create/update/delete activities performed by users are captured to support user access controls, troubleshooting, and incident response support.

M. What controls will be used to prevent unauthorized monitoring?

User accounts are reviewed annually and only authorized access is granted to designated users

through implementation/enforcement of record-level permissions that are assigned to users in groups. Unauthorized or inactive accounts are disabled. User accounts require authentication through use of DOI provided PIV card and PIN. User accounts are granted access to groups based on their need for access to specific cases and guest accounts are not permitted in ELRTS.

Access to administrative functions is strictly controlled and can only be granted by the ELRTS system administrators. System administrators periodically review audit logs to prevent any unauthorized monitoring. Users are also required to sign rules of behavior. All users must have a DOI account and government issued personal identity verification (PIV) card to access ELRTS. Technical controls such as firewalls, encryption, audit logs, least privileges, malware identification, and data loss prevention policies also help prevent unauthorized monitoring.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☒ Safes
☒ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits

☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Director, HR Information Systems serves as the ELRTS Information System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in ELRTS. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within ELRTS, in consultation with DOI Privacy Officials.

Each DOI bureau or office is responsible for the management of their own data, protecting the privacy rights of the employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act including any request for notification, access or amendment in consultation with privacy officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The ELRTS Information System Owner and is responsible for daily operational oversight and management of the security and privacy controls, for ensuring to the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The ELRTS Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and appropriate DOI officials in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the Departmental Privacy Officer.

System administrators and contractors are required to report any potential loss or compromise to the Information System Owner and Information System Security Officer. Each DOI bureau or office is responsible for the management of their own data, protecting the privacy rights of the employees for the information they collect, maintain, and use in the system, and for meeting the

requirements of the Privacy Act, and reporting any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data.