U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Labor and Employee Relations Information System (LERIS)

Responsible Official

Name: Victor Patino
Email: victor.patino@faa.gov
Phone Number: 202-267-4426

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Digital & Information Officer
privacy@dot.gov

Executive Summary

The Federal Aviation Administration's (FAA) Office of Human Resource Management (AHR), specifically the Office of Labor and Employee Relations (AHL), contracted with GDC Integration (GDCI) for the Labor and Employee Relations Information System (LERIS), which is a comprehensive workload tracking system for labor-management relations, employee relations matters, Employee Assistance Program activities, and for the tracking of official passports and visas. The information collected in the LERIS system is governed by the following authorities: 5 U.S.C. Ch. 71; 5 Code of Federal Regulations (CFR) Part 771; 22 U.S.C. 211a, DOT Policy Framework for the Prevention of Harassment, FAA Order 1110.125B and Equal Employment Opportunity (EEO) Management Directive (MD) 715.

The FAA conducted this Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002. While the LERIS system mainly maintains Personally Identifiable Information (PII) relating to individuals employed by or contracted with the Department of Transportation, PII on members of the public is collected during the passport and visa tracking process for employee dependents and in non-employee complaints received by and investigations conducted by the FAA's Accountability Board. The PIA is updated to reflect the system of records notices (SORNs) and records retention schedules that apply to the processes that are supported and other administrative items and to clarify content.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

[1] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The FAA, within the Department of Transportation (DOT), has been given the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. The FAA is responsible for:

- Regulating civil aviation to promote safety;
- Encouraging and developing civil aeronautics, including new aviation technology;
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- Regulating United States (U.S.) commercial space transportation.

One of the programs that helps the FAA fulfill this mission is LERIS, which is a case management system used by various groups under the FAA's AHR, as well as the labor and employee relations offices of the DOT. FAA's Employee Relations/Labor Relations (ER/LR) employees track, manage and report on labor and employee relations cases throughout the FAA. The LERIS system tracks work in progress and stores historical workload and case data for research and analysis. The system collects information to accurately identify employees involved in grievances and disciplinary actions.

The legal authority for information collection is 5 U.S.C. Chapter 71; 5 Code of Federal Regulations (CFR) Part 771; 22 U.S.C. 211a, DOT Policy Framework for the Prevention of Harassment, FAA Order 1110.125B and Equal Employment Opportunity (EEO) Management Directive (MD) 715. The ER/LR records on employees are retrievable by entering the employee's full name or a LERIS-generated employee case file number into a dialogue box to obtain all available information related to a case. The system validates entries with respect to the business rules, presents it for user verification and update, and allows information to be reported to upper management.

The initial data used within LERIS comes from a one-way exchange of information from the Consolidated Automated System for Time and Labor Entry/Interface Repository (CASTLE/IR), and no forms are used for this information. LERIS receives information from CASTLE/IR, which contains Federal Personnel/Payroll System (FPPS) data to prepopulate LERIS if employees need to use system services. This connection allows for the sharing of payroll related information for use in evaluating and administrating grievance cases and disciplinary actions. A Memorandum of Understanding (MOU) exists between LERIS and CASTLE/IR. The data pulled from CASTLE/IR includes: Full name, Date of Birth, Home Address, Work Email address, Work Address and FPPS ID. Additional Information from the Labor and Employee Relations (LER) Process for DOT employees includes: Medical information related to drug and alcohol abuse, misuse, treatment, control, and participation in rehabilitation programs and financial information (payroll data that includes wage, grade, pay plan, step status, and email address, if provided). For the passport and visa tracking process, the information collected includes passport numbers, passport issue and expiration dates, location and date of projected official travel and visa information.

LERIS is a web-based application offered by a General Services Administration (GSA) approved service provider, GDCI, a FedRAMP certified service provider. GDCI General Support System (GSS) hosts a suite of applications, including LERIS, which it provides to the FAA as a Software-as-a-Service.

System Functionality:

LERIS tracks information for the Accountability Board (AB) to provide oversight and ensure that management is accountable for responding to allegations of harassment generated by DOT federal employees. New AB records are initially populated with the FPPS data that is received via the CASTLE/IR connection. This feed auto-populates basic employee information into LERIS to include full name, line of business, position title, facility, organization, and date of birth (which may be used in age discrimination related allegations). Once the initial record is populated with the FPPS data, the AB receives the remainder of the record's data from the employee by having them complete an AB

Allegation Report Form or via a phone call, e-mail, fax, mail, walk-ins or the FAA Hotline. There is an approved Privacy Act Statement (PAS) on the AB Allegation form. Next, the appropriate Accountable Official (management) is notified so they can conduct an inquiry or security investigation into the matter and take appropriate action in response to the allegation. The inquiry and investigation results and management's response to the allegation (e.g. whether no action was taken, whether training was recommended, or whether there was disciplinary action) are provided to the AB who then enters the information into LERIS to meet the timelines established in FAA Order 1110.125B. Once the AB record contains management responses, those responses could add information about the employee's adverse actions, performance-based reduction in grade, and removal actions, termination decisions, or other performance indicators and/or reports that may result in engagement of ER/LR services or functions. The AB record could also include the names of judges and opposing attorneys involved in the adjudication process of any ER/LR cases.

LERIS application users (who comprise the Department's passport group) collect and track passport and visa information in LERIS on behalf of the Office of Policy, International Affairs and Environment. The passport group tracks passport and visa related actions to ensure they are completed and are reported to both the Office of the Secretary (OST) Security Office and the Department of State (DOS) for accounting and credentialing purposes. Both OST and DOS track the number of official passports processed in a fiscal year and the number of visas processed or cancelled in a fiscal year. The passport/visa records are initially created for DOT employees, traveling on official government business, within LERIS. Once the initial process of loading the employee data from the one-way connection from the CASTLE/IR populates the data, the passport group can then enter the individual's passport number, issue and expiration dates, location, dates of projected travel, and visa information. This additional data is obtained from signed passport applications and/or visa request forms, (not from CASTLE/IR feed), provided in person or through the mail by the employee. Finally, the passport group submits the completed hard copy applications to the DOS for passports and to embassies in the Washington D.C. area for visa requests.

LERIS sends the FAA employee/contractor FPPS ID, allegation type, type of discipline, non-disciplinary adverse action, incident date, offences information, number of prior offenses, proposed action, proposal issued date, final decision, number of suspension days, effective date of decision/action, disposition of decision, abeyance reason, case description, last updated, type of grievance, group grievance, union name, current step, grievance description, Opportunity to Demonstrate Performance (ODP) begin and end date, and outcome to the Office of Security & Hazardous Materials Safety (ASH) Wisdom Insider

Threat Information (ITI) in a one-way data push in order to build algorithms to identify potential insider threats.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

The authorities governing the operations and information collection include: 5 U.S.C. Ch. 71, 22 U.S.C. 211a, 5 CFR Part 771, DOT Policy Framework for the Prevention of Harassment, FAA Order 1110.125B and EEO MD 715.

The System of Records Notices (SORNs) governing retrieval of records by identifier(s) is as follows: DOT/ALL 1 *Grievance Records Files*, 65 FR 19478 (April 11, 2000); *OPM/GOVT 1, General Personnel Records,* 88 FR 56058 (August 17, 2023); OPM/GOVT 2, *Employee Performance File System Records*, 87 FR 5874 (February 02, 2022); OPM/GOVT-3 *Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers,* 87 FR 5874 (February 2, 2022); EEOC/GOVT 1, *Equal Employment Opportunity in the Federal Government Complaint and Appeals Records*, 67 FR 49338 (July 30, 2002) ; and MSPB/GOVT 1, *Appeals and Case Records,* 77 FR 65206 (October 25, 2012). The FAA published *DOT/FAA 859 Passport and Visa Tracking Records* that governs the retrieval of passport and visa tracking records and is working on another

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

SORN to govern the retrieval of the Accountability Board complaint and investigative records.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into LERIS.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Once the initial process of loading the employee data from the one-way connection from the CASTLE/IR populates the data, the passport group can then enter the individual's passport number, issue and expiration dates, location, dates of projected travel and visa information. This additional data is obtained from signed passport applications and/or visa request forms provided in person or through mail by the employee.

Under the provisions of the Privacy Act, individuals may request searches of LERIS to determine if any records have been added that may pertain to them. Individuals wishing to know if their records appear in these systems may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, SW
Washington, DC 20591

The request must include the following information:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records.

Contesting record procedures: Individuals wanting to contest information about themselves that is contained in LERIS should make their request in writing, detailing the reasons why their records should be corrected and addressing their letter to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, SW
Washington, DC 20591

Additional information about the Department's privacy program may be found at https://www.transportation.gov/privacy. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

LERIS tracks, manages and reports on labor and employee relations cases throughout the agency. The system tracks work in progress and stores historical workload and case data for research and analysis. LERIS collects information to accurately identify employees involved in grievances and disciplinary actions.

The authorities governing the operations and information collection in LERIS include: 5 U.S.C. Ch. 71, 5 CFR Part 771, 22 U.S.C. 211a, DOT Policy Framework for the Prevention of Harassment, FAA Order 1110.125B and EEO MD 715.

LERIS data retrieval is governed by the following SORNs: DOT/ALL 1 *Grievance Records Files*, 65 FR 19478 (April 11, 2000); OPM/GOVT 1, *General Personnel Records,* 80 FR 74815 (November 30, 2015); OPM/GOVT 2, *Employee Performance File System Records,* 80 FR 74815 (November 30, 2015); OPM/GOVT 3, *Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers,* 80 FR 74815 (November 30, 2015); EEOC/GOVT 1, *Complaint and Appeal Records,* 81 FR 81116 (November 17, 2016); MSPB/GOVT 1, *Appeals and Case Records,* 77 FR 65206 (October 25, 2012); DOT/FAA 859 *Passport and Visa Tracking Records*; and another SORN (to be determined) to cover Accountability Board records.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

LERIS collects the minimum amount of PII necessary to document the various LER operations that the system supports.

The system records are governed by the following retention schedules: 1) GRS 2.2 DAA-GRS-2017-0007-0013, Item 090: *Records Related to Official Passports*, Destroy when 3 years old or upon employee separation or transfer, whichever is sooner; but longer retention is authorized if required for business use; 2) GRS 2.3 DAA-GRS-2018-0002-0005, Item

050: *Harassment complaint case files*, Destroy 7 years after close of case, but longer retention is authorized if required for business use; 3) GRS 2.3 DAA-GRS-2018-0002-0006, Item 060: *Administrative grievance, disciplinary, performance-based, and adverse action case files*, Destroy no sooner than 4 years but no later than 7 years after case is closed or final settlement on appeal, as appropriate; 4) GRS 2.3 DAA-GRS-2018-0002-0009, Item 080: *Merit Systems Protection Board (MSPB) case files*, Destroy 3 years after final resolution of case, but longer retention is authorized if required for business use; 5) GRS 2.3 DAA-GRS-2018-0002-0010, Item 090*: Grievances, Appeals & Hearing Files*, Destroy 3 years after close of case, but longer retention is authorized if required for business use; 6) GRS 2.3 DAA-GRS-2018-0002-0011, Item 100: *Federal Labor Relations Authority (FLRA) case files*, Destroy 3 years after final resolution of case, but longer retention is authorized if required for business use; 7) GRS 2.3 DAA-GRS-2018-0002-0013, Item 111: *EEO Discrimination complaint cases files: Formal process*, Destroy 7 years after resolution of case, but longer retention is authorized if required for business use; 8) GRS 2.3 DAA-GRS-2018-0002-0015, Item 130: *Labor management relations agreement negotiation records. (Does not apply to nationally negotiated agreements. See Records Schedule NC1-237-77-04 -Approved 4/7/77)*, Destroy 5 years after expiration of agreement or final resolution of case, as appropriate, but longer retention is authorized if required for business use; 9) GRS 2.6 DAA-GRS-2016-0014-0001, Item 10: *Non-mission employee training program records*, Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use; 10) GRS 2.7 DAA-GRS-2017-0010-0014, Item 090: *Employee Assistance Program (EAP) records*, Destroy once employee has met condition(s) specified by agreement or adverse action or performance-based action case file has been initiated; and 11) NC1-237-77-04 (Approved 4/7/77), Item 003: *Labor Relations Agreements, Negotiations Files, Case files*, Permanent.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

FAA's Employee Relations/Labor Relations (ER/LR) employees use LERIS to track, manage, and report on labor and employee relations cases throughout the agency. LERIS tracks work in progress and stores historical workload and case data for research and analysis. The system collects information, especially PII, to accurately identify employees involved in grievances and disciplinary actions. LERIS receives data directly from FAA employees and others (i.e., employee dependents, complainants, witnesses) and internal feeds. There is no external sharing of LERIS data.

None of the SORNs governing LERIS contain system-specific routine uses. Both DOT/ALL 1 *DOT Grievance Records Files* and DOT/FAA 859 *Passports and Visa Tracking Records* SORNs include the 15 DOT-wide routine uses. The other government-wide SORNs contain their respective routine uses covering the respective record types.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

LERIS receives data from the Department of Transportation IR which interfaces with the National Business Center Federal Personnel/Payroll System (FPPS) and uses the FPPS DataMart. The accuracy of the data received is assumed from these databases. Case management data is entered by the appropriate LER specialists within the FAA. Manual data entry is aided by redlining typographical errors needing correction. There are date-formatted fields, pre-populated timelines based on impacted contract(s) and action fields with drop-down menus among other aides to ensure data quality and accuracy.

If inaccurate personal data is received by LERIS from FPPS via DOT IR, such data must be corrected in the FPPS database through procedures established for that system. Corrected data is then transferred to LERIS where the records are updated.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information

Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020 (includes updates as of December 10, 2020).

LERIS protects PII with reasonable administrative, technical, and physical security safeguards against loss or unauthorized access or compromise of the information. The system is only available to authorized FAA employees.

FAA personnel adhere to agency-wide procedures for handling and safeguarding PII and receive annual privacy and security training. The system manages access to information through user roles. Users receive the least privileges possible to perform their job duties through the user roles for development, support and maintenance. Additionally, LERIS administrators conduct initial user training as well as ad-hoc training by request. A system user guide is also available to all.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FAA Order 1370.121B, *"FAA Information Security and Privacy Program & Policy,"* implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance. DOT implements effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals. In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with LERIS are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of LERIS as related to the requirements of OMB Circular A-130, *"Managing Information as a Strategic Resource."*

Responsible Officials

Victor Patino
LERIS System Owner
Office of Labor and Employee Relations

Prepared by: Michael Bjorkman

Approval and Signature

Karyn Gorman
Chief Privacy Officer
KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2026.06.10 09:54:11 -04'00'
Office of the Chief Digital & Information Officer