Harper, Rains, Knight & Company

PERFORMANCE AUDIT REPORT

ON THE FEDERAL LABOR RELATIONS AUTHORITY'S PRIVACY AND DATA PROTECTION PROGRAM

FOR FISCAL YEAR 2026

REPORT NO. AR-26-05

Harper, Rains, Knight & Company, P.A.
1425 K Street NW, Suite 1120
Washington, D.C. 20005
202-558-5162
www.hrkcpa.com

Harper, Rains, Knight & Company

TABLE OF CONTENTS

Harper, Rains, Knight & Company

Independent Auditors' Performance Audit Report on the Federal Labor Relations Authority's Privacy and Data Protection Program for Fiscal Year 2026

The Honorable Colleen Duffy Kiko
Chairman
Federal Labor Relations Authority

Harper, Rains, Knight & Company was engaged by the Federal Labor Relations Authority (FLRA), Office of Inspector General (OIG), to conduct an independent performance audit of the FLRA's Privacy and Data Protection Program for Fiscal Year (FY) 2026. This report presents the results of our audit. Section 522 of Division H, Title V of the Consolidated Appropriations Act, 2005, as amended and codified at 42 U.S.C. § 2000ee-2, requires agencies to establish and implement comprehensive privacy and data protection procedures and requires the Inspector General to periodically review the agency's implementation and report the results to the Committees on Appropriations of the House of Representatives and the Senate, the House Committee on Oversight and Government Reform, and the Senate Committee on Homeland Security and Governmental Affairs. Additional privacy requirements applicable to FLRA include the Privacy Act of 1974, 5 U.S.C. § 552a; section 208 of the E-Government Act of 2002; and Office of Management and Budget (OMB) privacy guidance.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objective of this performance audit was to determine whether FLRA complied with applicable privacy and data protection laws, regulations, policies, and procedures for FY 2026. We concluded that FLRA complied with the privacy and data protection requirements applicable to the agency for FY 2026. Specifically, within the scope of our audit, FLRA maintained privacy governance and oversight, documented privacy policies and incident response procedures, public-facing privacy notices and privacy impact assessments for identified systems, and privacy training documentation for the audit period.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose. We appreciate the cooperation and courtesies that FLRA personnel extended to us during the execution of this performance audit.

Harper, Rains, Knight & Company, P.A.

May 11, 2026
Washington, DC

Certified Public Accountants · Consultants · hrkcpa.com

1052 Highland Colony Parkway, Suite 100
Ridgeland, MS 39157
p: 601-605-0722 · f: 601-605-0733

1425 K Street NW, Suite 1120
Washington, DC 20005
p: 202-558-5162 · f: 601-605-0733

Introduction

The privacy and data protection review required by 42 U.S.C. § 2000ee-2 complements, but does not replace, other federal privacy requirements. These requirements include the Privacy Act of 1974, which governs records maintained in systems of records; section 208 of the E-Government Act of 2002, which requires privacy impact assessments for applicable electronic information systems and collections; and OMB privacy guidance addressing privacy governance, privacy notices, training, and continuous monitoring.

Section 522 of Division H, Title V of the Consolidated Appropriations Act, 2005 requires agencies to establish and implement comprehensive privacy and data protection procedures governing the collection, use, sharing, disclosure, transfer, storage, and security of information in identifiable form relating to agency employees and the public. The statute also requires agencies to prepare a written benchmark report of their use of information in identifiable form and requires the Inspector General to periodically review the agency's implementation.

OMB guidance further requires agencies to designate a Senior Agency Official for Privacy with agency-wide responsibility and accountability for the privacy program; conduct privacy impact assessments when developing or procuring applicable information technology; maintain privacy policies on public-facing websites; and ensure that privacy training and privacy controls are sufficient to manage privacy risks.

Objective, Scope, and Methodology

The objective of this performance audit was to determine whether FLRA complied with applicable privacy and data protection laws, regulations, policies, and procedures for FY 2026.

We conducted this performance audit from January 2026 through April 2026. The scope was limited to FLRA privacy governance, policies, procedures, systems and documentation containing information in identifiable form, publicly available data and privacy notices on www.flra.gov and https://efile.flra.gov, and privacy training and incident documentation for FY 2026.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our objective, we interviewed FLRA management and reviewed privacy governance documentation, policies and procedures, privacy impact assessments, incident response and breach response documentation, training materials and completion evidence, public-facing privacy notices, and selected system and website documentation. We compared FLRA's privacy practices and documentation to applicable statutory and OMB criteria to identify any noncompliance or opportunities for improvement.

In performing the audit, we considered internal control for FLRA only to the extent necessary to satisfy the audit objective in planning our procedures. Our consideration of internal control would not necessarily have disclosed all privacy gaps or deficiencies that may have existed at the time of our audit. We assessed the reliability of the policies, procedures, data, and website information collected during the audit and determined that it was sufficiently reliable and valid for use in meeting the audit objective. We assessed the risk of fraud related to our audit objective while evaluating evidence and had no matters come to our attention indicating fraud or illegal acts were occurring.

We used the following criteria and procedures to determine compliance with FLRA's privacy practices. We took the following steps to accomplish the objective:

- Reviewed section 522 of Division H, Title V of the Consolidated Appropriations Act, 2005, as amended and codified at 42 U.S.C. § 2000ee-2; the Privacy Act of 1974, 5 U.S.C. § 552a; section 208 of the E-Government Act of 2002; OMB Circulars A-108 and A-130; OMB Memorandum M-03-22; and other applicable privacy guidance.
- Identified and reviewed applicable FLRA privacy policies, procedures, governance documentation, and prior privacy audit reports.
- Reviewed FLRA's public-facing privacy notices and publicly available privacy impact assessments for identified systems, including eFiling, the General Support System Network, E-Gov Travel Services 2, PRISM, and the Microsoft Office 365 Cloud Environment.
- Reviewed FLRA's public-facing websites, including www.flra.gov and https://efile.flra.gov, and performed procedures to identify potential public exposure of information in identifiable form.
- Reviewed privacy training materials, training completion documentation, incident response procedures, and breach response documentation for the audit period.

Results

Privacy Governance and Program Oversight

FLRA maintained a designated senior privacy official and supporting governance documentation during FY 2026. We reviewed organizational information, governance materials, privacy program communications, and related documentation to determine whether privacy roles and responsibilities were defined and communicated across the agency. Based on the procedures performed, we did not identify reportable deficiencies in FLRA's privacy governance and program oversight structure.

Privacy Policies, Procedures, and Public Notices

We reviewed FLRA's privacy policies and procedures against applicable criteria, including the Privacy Act, section 208 of the E-Government Act, and relevant OMB privacy guidance. Within the scope of our audit, FLRA maintained documented policies addressing the collection, use, safeguarding, retention, and incident reporting of personally identifiable information, and FLRA maintained public-facing privacy notices and links to applicable privacy impact assessments.

Governance	Policy	Privacy Impact Assessments (PIAs)	Website	Training/Incident Response
Compliant	Compliant	Compliant	Compliant	Compliant

The table above summarizes FLRA's compliance with the principal privacy areas tested.

Systems, Public Websites, and Publicly Available Information

We reviewed FLRA's public-facing websites, including www.flra.gov and https://efile.flra.gov, and performed procedures to identify potential public exposure of information in identifiable form. Based on the procedures performed, we did not identify reportable instances of public exposure of personally identifiable information or material inconsistencies between FLRA's public privacy notices and the practices reflected in the documentation reviewed. We also did not identify reportable exposure of personally identifiable information through the metadata procedures performed.

Privacy Training and Incident Response

We reviewed privacy training materials, training completion documentation, and incident and breach-response procedures for the audit period. Based on the procedures performed, FLRA maintained privacy training and incident response documentation within the scope of our audit, and management represented that FLRA had no reportable privacy breaches during the audit period.

Findings

No reportable findings were identified in the areas tested.

Conclusions

We determined FLRA was compliant with applicable privacy and data protection requirements for FY 2026 within the scope of our audit. FLRA maintained privacy governance and oversight, documented privacy policies and procedures, public-facing privacy notices and privacy impact assessments for identified systems, privacy training, and incident response documentation. Based on the procedures performed, we identified no reportable findings.

Appendix: Report Distribution

The Honorable Anne M. Wagner
Member
Federal Labor Relations Authority

The Honorable Charles Arrington
Member
Federal Labor Relations Authority

Dana Rooney
Inspector General
Federal Labor Relations Authority

Michael Jeffries
Executive Director
Federal Labor Relations Authority

Thomas Tso
Senior Agency Official for Privacy
Federal Labor Relations Authority

Director, Information Resources Management Division
Federal Labor Relations Authority