Harper, Rains, Knight & Company

PERFORMANCE AUDIT REPORT

ON THE FEDERAL LABOR RELATIONS AUTHORITY'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 (FISMA)

FOR FISCAL YEAR 2026

REPORT NO. AR-26-06

Harper, Rains, Knight & Company, P.A.
1425 K ST NW, Suite 1120
Washington, DC 20005
202-558-5163
www.hrkcpa.com

Harper, Rains, Knight & Company

TABLE OF CONTENTS

Independent Auditors' Performance Audit Report on the Federal Labor Relations Authority's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2026 1

Background 3

Objective, Scope, and Methodology 4

Results 7

Appendix A – Status of Prior Findings 8

Appendix B – Report Distribution 9

Harper, Rains, Knight & Company

INDEPENDENT AUDITORS' PERFORMANCE AUDIT REPORT ON THE FEDERAL LABOR RELATIONS AUTHORITY'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2026

The Honorable Colleen Duffy Kiko
Chairman
Federal Labor Relations Authority

This report presents the results of our independent performance audit of the Federal Labor Relations Authority's (FLRA) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires Federal agencies, including FLRA, to have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results of the evaluation to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). The FLRA Office of Inspector General (OIG) contracted with Harper, Rains, Knight & Company, PA (HRK) to conduct a performance audit of FLRA's information security program and practices for Fiscal Year (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, 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 assess the effectiveness of the FLRA's information security program and practices for FY 2026. As part of our audit, we responded to the core metrics and supplemental metrics identified in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (IG Metrics)* and the associated *FY 2025 Inspector General FISMA Metrics Evaluator's Guide*. As no changes were made to the IG FISMA Reporting Metrics for FY 2026, the FY 2025 Metrics remain the prevailing criteria. We assessed the maturity levels on behalf of the FLRA OIG to be managed and measurable, which we determined to be overall effective. The FLRA is a small, independent federal agency. As such, in some instances, the FLRA generally does not have the resources, or in some cases the need, to implement the extent of controls described at a level equal to or greater than "managed and measurable." We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and the NIST *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*.

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.

Washington, D.C.
July 16, 2026

Background

The Information Resources Management Division (IRMD) is responsible for planning, developing, implementing, and maintaining the Federal Labor Relation Authority's (FLRA) Information Technology (IT) program, policies, standards and procedures. IRMD promotes the application and use of information technologies and administers policies and procedures within FLRA to ensure compliance with related federal laws and regulations, to include information security. The Chief Information Officer (CIO) is the official responsible for carrying out the mission of the IRMD, which is responsible for designing the enterprise information architecture; determining the requirements of FLRA's information systems; and developing the integrated systems for nationwide use. Within the IRMD is the Chief Information Security Officer (CISO) who is the official responsible for carrying out the IRMD responsibilities under the Federal Information Security Modernization Act of 2014 (FISMA), including IT governance and security, and is the primary liaison to FLRA's authorizing officials, systems owners, and information security officials.

Federal Information Security Modernization Act of 2014[1]

FISMA codifies the Department of Homeland Security's (DHS) role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting the Office of Management and Budget (OMB) in developing those policies. The legislation provides DHS authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. FISMA also:

- Authorizes DHS to provide operational and technical assistance to other federal Executive Branch civilian agencies at the agency's request;
- Places the federal information security incident center (a function fulfilled by US-CERT) within DHS by law;
- Authorizes DHS technology deployments to other agencies' networks (upon those agencies' request);
- Directs OMB to revise policies regarding notification of individuals affected by federal agency data breaches;
- Requires agencies to report major information security incidents as well as data breaches to Congress as they occur and annually; and
- Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting while adding new reporting requirements for major information security incidents.

FISMA requires FLRA to develop, document, and implement an agency-wide information security program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also places responsibility on each agency program office to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.

[1] From overview section of the Cybersecurity & Infrastructure Security Agency's (CISA) FISMA page: https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

Furthermore, OIG must submit to DHS the "Inspector General FISMA Reporting Metrics" that depicts the effectiveness of the agency's information security program.

FISMA requires each agency inspector general (IG), or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders worked collaboratively to develop the *FY 2025 IG FISMA Reporting Metrics*. The *FY 2025 IG FISMA Reporting Metrics* represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle. As of the date of this report, no succeeding IG FISMA Reporting Metrics have been issued; therefore, the FY 2025 IG FISMA Reporting Metrics remain the applicable metrics for this FY 2026 audit.

The multi-year cycle for IG reporting metrics broke out metrics into two categories, core metrics and supplemental metrics. The core metrics represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine program effectiveness[2]. The supplemental metrics are considered core metrics but represent important activities conducted be security programs and contribute to the overall evaluation and determination of security program effectiveness. The supplemental metrics consist of five metrics designed to gauge the maturity of agencies' cybersecurity governance practices and implementation of key components of a Zero Trust Architecture. These five metrics will be evaluated by IGs and scored in FY 2026. IGs will consider the supplemental metric ratings when making the domain and function level maturity determinations[3].

The IG FISMA metrics, developed by and in coordination with OMB, CIGIE, and CIO and CISO councils, are aligned with the six function areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0: govern, identify, protect, detect, respond, and recover. The Cybersecurity Framework provides agencies with a common structure for managing and reducing their cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks[4].

Objective, Scope, and Methodology

The objective of this performance audit was to assess the effectiveness of the FLRA's information security program and practices for the period October 1, 2025, through June 30, 2026. As part of our audit, we responded to the core metrics identified in the *FY 2025 Inspector General FISMA Reporting Metrics*, the associated *FY 2025 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the FLRA OIG. We also considered applicable OMB policy and guidelines, NIST standards and guidelines, and the NIST *Cybersecurity Framework*.

[2] From FY 2025 IG FISMA Metrics Evaluator's Guide introduction section, core metrics definition: https://www.cisa.gov/sites/default/files/2025-05/Final%20FY%202025%20IG%20FISMA%20Metrics%20Evaluation%20Guide_05%20May%202025-508.pdf
[3] From FY 2025 IG FISA Metrics Evaluator's Guide introduction section, supplemental metrics definition: Ibid.
[4] Background from the FY 2025 IG FISMA Reporting Metrics, General Instructions section: https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508_0.pdf

To address our audit objective, we assessed the overall effectiveness of the FLRA information security program and practices in accordance with Inspector General reporting requirements:

- Cybersecurity Governance (Govern)
- Cybersecurity Supply Chain Risk Management (Govern)
- Risk and Asset Management (Identify);
- Configuration Management (Protect);
- Identity and Access Management (Protect);
- Data Protection and Privacy (Protect);
- Security Training (Protect);
- Information Security Continuous Monitoring (Detect);
- Incident Response (Respond); and
- Contingency Planning (Recover).

We conducted this 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.

We performed procedures to determine the status of recommendations from prior FISMA audits (see ***Appendix A***).

We reviewed FLRA's general FISMA compliance efforts in the specific areas defined in DHS guidance and the corresponding reporting instructions. We considered the internal control structure for FLRA's systems in planning our audit procedures. Accordingly, we obtained an understanding of the internal controls over FLRA's systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. When appropriate, we conducted tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish our audit objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to FLRA's information security program, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected controls;
- Reviewed the status of recommendations in prior year FISMA audit reports;

The independent performance audit was conducted from February 23, 2026 through July 31, 2026. It covered the period from October 1, 2025, through June 30, 2026.

Criteria

The criteria used in conducting this audit included:

- Public Law. 113-283, *Federal Information Security Modernization Act of 2014*;

- FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 2.0, April 3, 2025;
- FY 2025 IG FISMA Metrics Evaluator's Guide, Version 1.0, May 5, 2025;
- OMB Circular A-123, *Management's Responsibility for Internal Control*;
- OMB Circular A-130, *Managing Information as a Strategic Resource*;
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*;
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*;
- OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*;
- OMB Memorandum M-21-30, *Protecting Critical Software through Enhanced Security Measures*;
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*;
- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*;
- OMB Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*;
- OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*;
- OMB Memorandum M-26-05, *Adopting a Risk-Based Approach to Software and Hardware Security*;
- OMB Memorandum M-26-14, *Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats*;
- Executive Order 14028, *Improving the Nation's Cybersecurity*;
- Executive Order 14144, *Strengthening and Promoting Innovation in the Nation's Cybersecurity, as amended*;
- DHS/CISA Binding Operational Directives and Emergency Directives, as applicable;
- Federal Acquisition Supply Chain Security Act of 2018;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- NIST Cybersecurity Framework, Version 2.0;
- NIST SP 800-12, Rev. 1, *An Introduction to Information Security*;
- NIST SP 800-18, Rev. 2, *Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems*;
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*;
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*;
- NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*;
- NIST SP 800-53A, Rev. 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*;

- NIST SP 800-61, Rev. 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*;
- NIST SP 800-63-4, *Digital Identity Guidelines*;
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*;
- NIST SP 800-161, Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*;
- NIST SP 800-207, *Zero Trust Architecture*;
- NIST SP 800-218, *Secure Software Development Framework*, as applicable;
- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- FIPS Publication 201-3, *Personal Identity Verification of Federal Employees and Contractors*;
- Federal Identity, Credential, and Access Management guidance, including the Federal ICAM Architecture and related implementation guidance; and
- Other criteria as appropriate.

Results

We assessed FLRA's information security program to be Managed and Measured, which we concluded was effective. The results of our independent performance audit concluded that FLRA's information security program is generally compliant with the FISMA legislation and is consistent with the functional areas outlined in the NIST Cybersecurity Framework.

The summary assessment results for FLRA maturity level assessment by function areas are in ***Exhibit 1***. The five maturity model levels are *ad hoc*, *defined*, *consistently implemented*, *managed and measurable*, and *optimized.*

Exhibit 1 – FLRA Overall Maturity Level Assessment by Functions Area for Core Metrics

FISMA NIST Cybersecurity Framework Functions Area	FY 2026 Maturity Level (Core & Supplemental Metrics)
Govern – Cybersecurity Governance and Supply Chain Risk Management	Level 4 - Managed and Measurable
Identify – Risk Management and Supply Chain Risk Management	Level 4 - Managed and Measurable
Protect – Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training	Level 4 - Managed and Measurable
Detect – Information Security Continuous Monitoring	Level 4 - Managed and Measurable
Respond – Incident Response	Level 4 - Managed and Measurable
Recover – Contingency Planning	Level 4 - Managed and Measurable

Ratings in FY 2026 will focus on a calculated average approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (govern, identify, protect, detect, respond, and recover) and the overall program.

Appendix A – Status of Prior Findings

No.	Prior Year Evaluation Recommendation	Status
1	**Report MAR-24-07 FISMA Recommendation No. 4**: Implement qualitative or quantitative measures to measure, report on, and monitor the information security and SCRM performance of organizationally defined products, systems, and services provided by external providers.	Closed

Appendix B – Report Distribution

Federal Labor Relations Authority

The Honorable Ann M. Wagner, Member
The Honorable Charles Arrington, Member
Executive Director
Chief Information Officer
Solicitor