Office of Inspector General

EVALUATION OF THE FEDERAL LABOR
RELATIONS AUTHORITY'S COMPLIANCE WITH
THE FEDERAL INFORMATION SECURITY
MODERNIZATION ACT OF 2014
FISCAL YEAR 2025

EVALUATION OF THE FEDERAL LABOR RELATIONS AUTHORITY'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

FISCAL YEAR 2025

Report No. MAR-25-09
JULY 2025

Federal Labor Relations Authority
1400 K Street, N.W., Washington, D.C. 20424

IMPORTANT NOTICE

This report contains sensitive content. The sensitive content is being withheld from public release due to concerns about the risk of circumvention of law.

CONTENTS

Evaluation Report

Appendices

Abbreviations

FISMA	Federal Information Security Modernization Act of 2014
FLRA	Federal Labor Relations Authority
FY	Fiscal Year
IG	Inspector General
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
Rocha	Rocha & Company, PC
SCRM	Supply Chain Risk Management

Rocha & Company, PC

Certified Public Accountants
and Management Consultants

Evaluation of the Federal Labor Relations Authority's Compliance with the Federal Information Security Modernization Act of 2014, Fiscal Year 2025

Report No. MAR-25-09 ***July 30, 2025***

The Honorable Colleen Duffy Kiko
Chairman

Rocha & Company, PC (Rocha), under contract with Dembo Jones, P.C., on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General (OIG), conducted an independent evaluation of the quality and compliance of the FLRA security program with applicable Federal computer security laws and regulations. Rocha's evaluation focused on FLRA's information security required by the Federal Information Security Modernization Act of 2014, as amended (FISMA). Any weaknesses discussed in this report should be included in FLRA's Fiscal Year (FY) 2025 report to the Office of Management and Budget (OMB) and Congress.

Results in Brief

During our FY 2025 evaluation, we noted that the FLRA has taken significant steps to improve the information security program by closing all prior year recommendations from the FY 2024 FISMA evaluation, with the exception of one (metric 14). We also noted there was one metric from the current year (metric 5) that was determined to be "not effective;" however, a new finding was not drafted since metric 5 was formerly metric number 14. The overall maturity level of the FLRA's information security program was determined as managed and measurable (Level 4), effective. We provided the FLRA a draft of this evaluation report for comment and management disagreed in part. *See* Management's Response in its entirety in Appendix III.

Report Findings

We reviewed selected controls including 20 Core and 5 Supplemental Inspector General FISMA Reporting Metrics. We also followed up on all prior year findings. This was accomplished by evaluating the six National Institute of Standards and Technology (NIST) Cybersecurity Framework functions:

- Govern, which includes organizational context and risk management;
- Identify, which includes risk management and supply chain risk management;
- Protect, which includes configuration management, identity and access management, data protection and privacy, and security training;
- Detect, which includes information security continuous monitoring;
- Respond, which includes incident response; and,
- Recover, which includes contingency planning.

We assessed the effectiveness of the agency's information security program and the maturity level of each functional area. The answers to the 20 Core and 5 Supplemental Inspector General FISMA Reporting Metrics in Appendix II reflect the results of our testing of the FLRA's information security program and practices.

The Core FISMA Metrics classify information and security programs and practices into five maturity levels: Level 1: Ad-hoc, Level 2: Defined, Level 3: Consistently Implemented, Level 4: Managed and Measurable, and Level 5: Optimized. A functional information security area is not considered effective unless it achieves a rating of at least Managed and Measurable (Level 4).

The Inspector General Evaluation Maturity Levels Table below summarizes the overall assessed maturity levels for each functional area and domain in the FY 2025 Inspector General FISMA Reporting Metrics.

Inspector General Evaluation Maturity Levels

Function and Domain Areas	FY 25 Core and Supplemental Assessed Maturity Levels
1. Govern – Cybersecurity Governance and Supply Chain Risk Management	Level 3 – Consistently Implemented
2. Identify – Risk Management and Supply Chain Risk Management	Level 5 – Optimized
3. Protect – Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training	Level 4 – Managed and Measurable
4. Detect – Information Security Continuous Monitoring	Level 4 – Managed and Measurable
5. Respond - Incident Response	Level 4 – Managed and Measurable
6. Recover - Contingency Planning	Level 5 – Optimized

Based on the results of our evaluation and analysis as determined by Cyberscope, we have deemed the overall maturity level to be 'Effective.'

Background

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of the E-Government Act of 2002, as amended, commonly referred to as FISMA,[1] focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires Federal agencies to develop, document, and implement an agency-wide

[1] Federal Information Security Modernization Act of 2014, Pub L. No. 113-283, 128 Stat. 3073.

information security program that provides security for the information and information systems that support the operations and assets of the agency. This program includes providing security for information systems provided or managed by another agency, contractor, or other source. FISMA assigns specific responsibilities to agency heads and Inspectors General (IG). It is supported by security policy promulgated through OMB, and risk-based standards and guidelines published in the NIST Special Publication series.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. FISMA directs Federal agencies to report annually to the OMB Director, Comptroller General, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB.[2] FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG. Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission. The IG plays an essential role in supporting Federal agencies in identifying areas for improvement. In support of that critical goal the FLRA supports the development of a strategy to secure the FLRA computing environment which centers on providing confidentially, integrity, and availability.

Scope and Methodology

The scope of our testing focused on the FLRA network General Support System; however, the testing also included all supporting major applications in the FLRA system inventory. We conducted our testing through inquiry of FLRA personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. Some examples of our inquiries with FLRA management and personnel included, but were not limited to, reviewing system security plans, access control, the risk assessments, and the configuration management processes. Specifically, we performed the following:

- Researched laws and regulations as well as other Federal guidance relating to FISMA.
- Interviewed information technology personnel.
- Reviewed and examined several artifacts supporting the FISMA evaluation.

[2] 44 U.S.C. § 3555.

This evaluation was conducted in accordance with the *Quality Standards for Inspection and Evaluation* (December 2020), issued by the Council of the Inspectors General on Integrity and Efficiency.

Management Response

A draft copy of this report was provided to the Director, Information Resources Management Division and the Executive Director. The Executive Director provided a formal response. With regards to recommendation (No. 4.), the Executive Director stated, "FLRA believes we have made significant strides in addressing it based on the previous year's report. While this year's report indicates that the "Govern" function—specifically, Cybersecurity Governance and Supply Chain Risk Management (SCRM)—is "Consistently Implemented," we believe that the actions taken by FLRA did address the specifics of last year's recommendation."

Evaluation of Management's Comments

We disagree. The assessment conducted by Rocha found that qualitative and quantitative measures to measure, report on, and monitor the information security and SCRM performance provided by external providers, was not evident from our evaluation.

Rocha & Company, PC

Rocha & Company, P.C.
Gaithersburg, Maryland
July 30, 2025

Appendix I
Prior Year Findings Status

Functional Area 1A – Identify – Risk Management			
Recommendation Number	**Recommendation**	**2024 IG Metrics Reference**	**Open / Closed**
1	Perform a risk-based allocation of resources based on system categorization.	4	Closed
2	Incorporate the system level risk assessment results into the organization-wide cybersecurity and privacy risk assessment.	5	Closed
3	Integrate the information security architecture with the development lifecycle.	6	Closed
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.**	**14**	**Open**

Functional Area 1B – Identify – Supply Chain Risk Management			
Recommendation Number	**Recommendation**	**2024 IG Metrics Reference**	**Open / Closed**
5	Implement qualitative or quantitative measures used to gauge the effectiveness of its component authenticity policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	15	Closed

Appendix I
Prior Year Findings Status

Functional Area 2A – Protect – Configuration Management			
Recommendation Number	**Recommendation**	**2024 IG Metrics Reference**	**Open / Closed**
6	Allocate resources in a risk-based manner.	17	Closed
7	Implement qualitative or quantitative measures on the effectiveness of the configuration management plan.	18	Closed
8	Ensure flaw remediation is centrally managed.	21	Closed
9	Implement qualitative or quantitative measures on the effectiveness of change control activities.	23	Closed

Functional Area 2B – Protect – Identify and Access Management			
Recommendation Number	**Recommendation**	**2024 IG Metrics Reference**	**Open / Closed**
10	Deploy automation to centrally document, track, and share risk designations and screening information with necessary parties.	28	Closed
11	Deploy automation to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.	32	Closed

Appendix I
Prior Year Findings Status

Functional Area 2C – Protect – Data Protection and Privacy			
Recommendation Number	**Recommendation**	**2024 IG Metrics Reference**	**Open / Closed**
12	The FLRA should ensure that the security controls for protecting Personally Identifiable Information and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's Information Security Continous Monitoring (ISCM) strategy.	36	Closed
13	Implement qualitative or quantitative measures on the performance of data exfiltration and enhanced network defenses.	37	Closed
14	Implement qualitative or quantitative measures on the effectiveness of the Data Breach Response Plan.	38	Closed
15	Obtain feedback from privacy training.	39	Closed

Functional Area 2D – Protect – Security Training			
Recommendation Number	**Recommendation**	**2024 IG Metrics Reference**	**Open / Closed**
16	Assess training and talent of workforce.	42	Closed
17	Obtain feedback regarding training needs of workforce.	45	Closed

Appendix I
Prior Year Findings Status

Functional Area 3 – Detect – ISCM			
Recommendation Number	**Recommendation**	**2024 IG Metrics Reference**	**Open / Closed**
18	Implement qualitative or quantitative measures on the effectiveness of the ISCM policies and strategy.	47	Closed

Functional Area 4 – Respond – Incident Response			
Recommendation Number	**Recommendation**	**2024 IG Metrics Reference**	**Open / Closed**
19	Implement qualitative or quantitative measures that have been defined in the Incident Response Plan to monitor and maintain the effectiveness of an overall incident response capability.	52	Closed
20	Perform risk-based allocation for stakeholders to effectively implement incident response activities.	53	Closed
21	Implement qualitative or quantitative measures to ensure the effectiveness of incident detection and analysis policies and procedures.	54	Closed
22	FLRA should monitor and analyze qualitative and quantitative performance measures on the effectiveness of incident handling policies and procedures.	55	Closed
23	Incident response metrics should be used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.	56	Closed

Appendix I
Prior Year Findings Status

Functional Area 5 – Recover – Contingency Planning			
Recommendation Number	**Recommendation**	**2024 IG Metrics Reference**	**Open / Closed**
24	FLRA should employ automated mechanisms to test system contingency plans more thoroughly and effectively.	63	Closed
25	Assess backups.	64	Closed

The subsequent section of the report is not being publicly released due to concerns about the risk of circumvention of law:

Appendix II: OIG Responses Reported in Cyberscope (pages 10-24).

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY

July 28, 2025

MEMORANDUM

TO: Dana Rooney, Inspector General

FROM: Dave Fontaine, Director Information Resources Management Division

THROUGH: Michael Jeffries, Executive Director

SUBJECT: Management Response to FY2025 Draft Report on the FLRA’s Compliance with the Federal Information Security Management Act

Thank you for the opportunity to review and provide comments on the Office of Inspector General’s (OIG) draft Evaluation of FLRA’s Compliance with the FISMA FY 2025, Report No. MAR-25-09. The Federal Labor Relations Authority (FLRA) appreciates the in-depth review of our information security program.

The Agency is very pleased with the assessment of an overall maturity Level 4 and the opinion that our IT security program is “effective.” We also appreciate the closure of 24 of the 25 open recommendations from last year’s report.

FLRA prioritizes its limited human and financial resources using our Risk Management Strategy as a roadmap. This approach allows us to effectively mitigate the most significant risks to our information systems and data. Despite our constraints as a small agency, we remain committed to improving our cybersecurity posture.

Regarding the remaining open finding, FLRA believes we have made significant strides in addressing it based on the previous year’s report. While this year’s report indicates that the “Govern” function—specifically, Cybersecurity Governance and Supply Chain Risk Management (SCRM)—is “Consistently Implemented,” we believe that the actions taken by FLRA did address the specifics of last year’s recommendation.

Specifically, in response to the sole open 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.”

FLRA has taken numerous actions, including fully adopting and integrating several new policies and supporting workflows into both the IT and contracts/acquisitions environments—policies that include the tools and mechanisms to measure, report on, and monitor the effectiveness of SCRM performance as recommended.

FLRA acknowledges that there is still work to be done to address new and evolving aspects of SCRM, such as Cybersecurity Supply Chain Risk Management (C-SCRM), which was a new focus of this year’s evaluation. The progress we made in addressing last year’s recommendations will support our continuing efforts. However, we believe that advancing from “Consistently Implemented” to “Managed and Measurable” in this updated domain will require a significant investment of resources. In accordance with our Risk Management Strategy, we have analyzed the risks of not funding these enhancements and determined that our current IT environment and security program present an acceptable level of risk in this area. Nevertheless, the FLRA will continue to explore alternative options - such as support from Department of Homeland Security (DHS) or future Department of Government Efficiency (DOGE) initiatives - that may enable us to implement these solutions more cost-effectively through economies of scale.

As always, we appreciate the recommendations of the Office of Inspector General and remain committed to achieving an effective and efficient IT security program at the FLRA.

Appendix IV
Report Distribution

Federal Labor Relations Authority

The Honorable Colleen Duffy Kiko, Chairman
The Honorable Ann M. Wagner, Member
Executive Director
Chief Information Officer
Solicitor

Contacting the Office of Inspector General

IF YOU BELIEVE AN ACTIVITY IS WASTEFUL, FRAUDULENT, OR ABUSIVE OF FEDERAL FUNDS, CONTACT THE:

HOTLINE (877) 740-8278

HTTP://WWW.FLRA.GOV/OIG-Hotline

CALL: (771) 444-5712 FAX: (202) 208-4535
WRITE: 1400 K Street, N.W.
Washington, D.C. 20424

The complainant may remain confidential; allow their name to be used; or anonymous. If the complainant chooses to remain anonymous, FLRA OIG cannot obtain additional information on the allegation, and also cannot inform the complainant as to what action FLRA OIG has taken on the complaint. Confidential status allows further communication between FLRA OIG and the complainant after the original complaint is received. The identity of complainants is protected under the provisions of the Whistleblower Protection Act of 1989 and the Inspector General Act of 1978. To learn more about the FLRA OIG, visit our Website at http://www.flra.gov/oig

Office of Inspector General

EVALUATION OF THE FEDERAL LABOR RELATIONS AUTHORITY'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014
FISCAL YEAR 2025