Office of Inspector General

EVALUATION OF THE FEDERAL LABOR RELATIONS AUTHORITY'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FISCAL YEAR 2024

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

FISCAL YEAR 2024

Report No. MAR-24-07
AUGUST 2024

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

Dembo Jones	Dembo Jones, P.C.
FISMA	Federal Information Security Modernization Act of 2014
FLRA	Federal Labor Relations Authority
FY	Fiscal Year
IG	Inspector General
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	NIST Special Publication Series

DEMBO·JONES
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Evaluation of FLRA's Compliance with the FISMA FY 2024

Report No. MAR-24-07 ***August 5, 2024***

The Honorable Susan Tsui Grundmann
Chairman

Dembo Jones, P.C. (Dembo Jones), 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. Dembo Jones' evaluation focused on FLRA's information security required by the Federal Information Security Modernization Act of 2014 (FISMA). Any weaknesses discussed in this report should be included in FLRA's Fiscal Year (FY) 2024 report to the Office of Management and Budget (OMB) and Congress.

Results in Brief

During our FY 2024 evaluation, we noted that the FLRA has taken significant steps to improve the information security program by closing the one prior year recommendation. The overall maturity level of the FLRA's information security program was determined as consistently implemented (Level 3), not effective. To receive an effective level of security, FLRA would need to achieve a rating of at least a Managed and Measurable (Level 4). We made 25 recommendations to assist FLRA in strengthening its information security program. See recommendations contained in Appendix I. We provided the FLRA a draft of this report for comment. While management agrees with the goal of achieving an overall maturity level 4, they do not agree with the determination that the information security program is not effective. See Management's Response in its entirety in Appendix IV.

Report Findings

We reviewed selected controls including 20 Core and 17 Supplemental Inspector General FISMA Reporting Metrics by evaluating the five National Institute of Standards and Technology (NIST) Cybersecurity Framework functions:

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

6116 Executive Blvd • Suite 500
North Bethesda, MD 20852
P 301.770.5100 • F 301.770.5202

Dembo Jones, P.C.
A Member of Allinial Global
www.dembojones.com

8830 Stanford Blvd • Suite 290
Columbia, MD 21045
P 410.290.0770 • F 410.290.0774

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 17 Supplemental Inspector General FISMA Reporting Metrics in Appendix III 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 function area and domain in the FY 2024 Inspector General FISMA Reporting Metrics.

Inspector General Evaluation Maturity Levels

Function and Domain Areas	FY 24 Core and Supplemental Assessed Maturity Levels
1. Identify – Risk Management and Supply Chain Risk Management	Consistently Implemented (Level 3)
2. Protect – Configuration Management, Identity and Access Management, Data Protection and Privacy and Security Training	Consistently Implemented (Level 3)
3. Detect – Information Security Continuous Monitoring	Managed and Measurable (Level 4)
4. Respond - Incident Response	Consistently Implemented (Level 3)
5. Recover - Contingency Planning	Managed and Measurable (Level 4)
Overall Effectiveness Rating – Not effective	Consistently Implemented (Level 3) Overall Maturity Core 3.56 and Supplemental 3.43

Two out of five functions met the managed and measurable (Level 4), with three consistently implemented (Level 3). We assessed FLRA's overall maturity level for the data protection and privacy program as Consistently Implemented (Level 3), not effective. OMB believes that achieving the Managed and Measurable (Level 4) or above represents an effective level of security.

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

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

Federal agencies to develop, document, and implement an agency-wide 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 (IGs). It is supported by security policy promulgated through OMB, and risk-based standards and guidelines published in the NIST Special Publication (SP) 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.

To further emphasize the importance of protecting critical infrastructure, Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017, was issued to hold agency heads accountable for managing cybersecurity risk in their organizations. Specifically, Executive Order 13800 requires agency heads to lead integrated teams of senior executives with expertise in information technology, security, budgeting, acquisition, law, privacy, and human resources. Furthermore, Executive Order 13800 states agency heads will be held accountable for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. They will also be held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.

[2] 44 U.S.C. § 3555.

Scope and Methodology

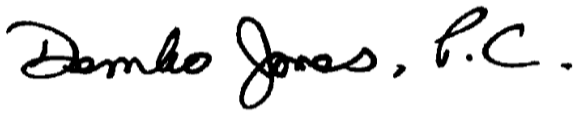
The scope of our testing focused on the FLRA network General Support System; however, the testing also included the other systems in the FLRA system inventory. We conducted our testing through inquiry of FLRA personnel, observation of activities, inspection of relevant documentation, and the performance 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.

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. FLRA non-concurred with the assessment that the security system program was *not* effective. The Executive Director asserted that the while FLRA's maturity level is at Level 3, FLRA believes that the security system *is* effective. The Executive Director stated that with its given resources and real-world challenges, the FLRA has demonstrated its information security program is effective.

Evaluation of Management's Comments

We disagree with the Executive Director's assertion that the FLRA's information security program is effective. The assessment conducted by Dembo Jones concluded that the FLRA has not shown that it has established an effective information security program and practices in line with FISMA requirements. Dembo Jones rated the FLRA at Level 3: Consistently Implemented, indicating that while policies, procedures, and strategies are consistently implemented; there is a lack of both quantitative and qualitative effectiveness measures. Dembo Jones made 25 recommendations with a goal to elevate the FLRA to Level 4: Managed and Measurable, which involves collecting and utilizing quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies across the organization and used to assess them and make necessary changes. The Executive Director's response did not address these recommendations. However, FLRA has indicated a commitment to advancing to a maturity level 4. Consequently, we consider management's lack of response to the recommendations as unresolved. We believe that the findings and conclusions of the report support our call for management's attention, and we will keep the recommendations open. Additionally, we request that management create a plan of action and milestones to achieve a maturity level 4 for its information security program.



Dembo Jones, P.C.
North Bethesda, Maryland
August 5, 2024

Appendix I
Recommendations

We recommend that the Director, Information Resources Management Division implement the following recommendations:

Functional Area 1A: Identify—Risk Management

NO.	RECOMMENDATION	IG METRICS REFERENCE
1	Perform a risk-based allocation of resources based on system categorization.	4.
2	Incorporate the system level risk assessment results into the organization-wide cybersecurity and privacy risk assessment.	5.
3	Integrate the information security architecture with the development lifecycle.	6.
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.

Functional Area 1B: Identify—Supply Chain Risk Management

NO.	RECOMMENDATION	IG METRICS REFERENCE
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.

Functional Area 2A Protect—Configuration Management

NO.	RECOMMENDATION	IG METRICS REFERENCE
6	Allocate resources in a risk-based manner.	17.
7	Implement qualitative or quantitative measures on the effectiveness of the configuration management plan.	18.
8	Ensure flaw remediation is centrally managed.	21.
9	Implement qualitative or quantitative measures on the effectiveness of change control activities.	23.

Appendix I
Recommendations

Functional Area 2B Protect—Identify and Access Management

NO.	RECOMMENDATION	IG METRICS REFERENCE
10	Deploy automation to centrally document, track, and share risk designations and screening information with necessary parties.	28.
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.

Functional Area 2C Protect—Data Protection and Privacy

NO.	RECOMMENDATION	IG METRICS REFERENCE
12	The FLRA should ensure that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.	36.
13	Implement qualitative or quantitative measures on the performance of data exfiltration and enhanced network defenses.	37.
14	Implement qualitative or quantitative measures on the effectiveness of the Data Breach Response Plan.	38.
15	Obtain feedback from privacy training.	39.

Functional Area 2D Protect—Security Training

NO.	RECOMMENDATION	IG METRICS REFERENCE
16	Assess training and talent of workforce.	42.
17	Obtain feedback regarding training needs of workforce.	45.

Functional Area 3 Detect—ISCM

NO.	RECOMMENDATION	IG METRICS REFERENCE
18	Implement qualitative or quantitative measures on the effectiveness of the ISCM policies and strategy.	47.

Appendix I
Recommendations

Functional Area 4 Respond—Incident Response

NO.	RECOMMENDATION	IG METRICS REFERENCE
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.
20	Perform risk-based allocation for stakeholders to effectively implement incident response activities.	53.
21	Implement qualitative or quantitative measures to ensure the effectiveness of incident detection and analysis policies and procedures.	54.
22	FLRA should monitor and analyze qualitative and quantitative performance measures on the effectiveness of incident handling policies and procedures.	55.
23	Incident response metrics should be used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.	56.

Functional Area 5 Recover—Contingency Planning

NO.	RECOMMENDATION	IG METRICS REFERENCE
24	FLRA should employ automated mechanisms to test system contingency plans more thoroughly and effectively.	63.
25	Assess backups.	64.

Appendix II
Prior Year Finding Status

As part of our review, we conducted follow-up steps regarding the open recommendation from last year. The recommendation was:

1. The FLRA should develop, review and update, as necessary, the following information security program policies and procedures in accordance with NIST and agency requirements:
    a. Personnel Security policy.
    b. Security Assessment policy.
    c. Identification and Authentication policy.
    d. Access policy.

During the review we obtained four pieces of evidence that were used to make the determination that the noted deficiencies are considered closed. The Policies obtained were as follows:

- Personnel Security Policy
- Security Assessment Policy
- Identification and Authentication Policy
- Access Control Policy

Based on review of the policies noted above, as well as interview with the Chief Information Officer, it was determined that the policies were adequate and met the guidelines proposed in the NIST Special Publications.

FY 2024 Status:

Closed

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

Appendix III: OIG Responses Reported in Cyberscope (pages 9-36).

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY

July 31, 2024

MEMORANDUM

TO: Dana Rooney, Inspector General

FROM: Dave Fontaine, Director Information Resources Management Division

THROUGH: Michael Jeffries, Executive Director

SUBJECT: Management Response to FY2024 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 2024, Report No. MAR-24-07. The Federal Labor Relations Authority (FLRA) appreciates the in-depth review of our information security program. We are pleased to have closed last year's open finding. The Agency concurs with the goal of achieving an overall maturity level 4. However, we do not agree with the general assumption that our program is ineffective solely because it has not yet achieved level 4.

We believe it is important to note that a maturity level 3 means that, generally, "[p]olicies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking."[1] While a maturity level at Level 4 or above represents "an effective level of security."[2] A maturity level below a Level 4 does not necessarily represent an ineffective level of security. "IGs should consider both their and the agency's assessment of unique missions, resources, and challenges when determining information security program effectiveness. . . . Therefore, an IG has the discretion to determine that an agency's information security program is effective even if the agency does not achieve a Level 4[.]"[3] Accordingly, the Agency implements a NIST-recommended, risk-based approach to information technology and cybersecurity (ITC), taking into account our missions, resources, and challenges. "IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency and to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls."[4] This approach allows us to prioritize our limited human and financial resources and 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.

[1] CISA, FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (February 10, 2023), available at https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf.
[2] *Id.*
[3] *Id.*
[4] CISA, FY 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics, Evaluator's Guide, available at https://www.cisa.gov/sites/default/files/2024-05/FY%202024%20IG%20FISMA%20Metrics%20Evaluation%20Guide%20Final.pdf.

Notably, during the past year, we successfully demonstrated our effectiveness in managing two major incidents. These incidents tested our readiness and response capabilities and validated, in real-world circumstances, the robustness of our current processes. While we believe, given our mission, resources and challenges, that we have an effective program, we will strive to achieve an overall maturity Level 4.

It is important also to provide some overall context. In FY 2023, for some of the larger twenty-three federal agencies, fifteen of those agencies had "not effective" ratings, and only eight had "effective" ratings. Only three agencies received an overall rating of Level 4, and thirteen received a rating of Level 2. Four agencies received an overall rating of Level 3 and were still considered "effective." One agency received an overall rating of Level 2 and was considered "effective."[5] As with the rest of the federal government, we will continue to maximize our resources to move towards an overall rating of Level 4 in the future.

We value the support and guidance provided by the Inspector General's office. Moving forward, we will continue to work closely with your team to identify areas for improvement and implement necessary changes. Your feedback is crucial in helping us strengthen our cybersecurity measures and achieve our goals. We understand your recommendations reiterate the broad standards stated in the metrics and we agree with the broad standards described in the metrics. In working with the Inspector General's office to raise FLRA's maturity level to Level 4, we believe:

> [R]ecommendations should be written from the perspective of what level the organization is at for the metric, and what it would take to progress to the next level. As a general best practice, broad recommendations should be avoided. Recommendations should be focused on specific actions to address the root cause and lead the agency to that next maturity level. It may require several recommendations to get that metric to the next level, however this provides the agency with specific guidance and the opportunity to make steady and visible progress.[6]

We welcome such recommendations in the future and will work with the Inspector General's Office on your future recommendations.

Thank you for your continued collaboration and support.

[5] "FY2023 Annual Cybersecurity Performance Summary," *available at* FY2023FISMAAnnualAgencyPerformanceSummaries.pdf (whitehouse.gov).
[6] CISA, FY 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics, Evaluator's Guide, available at https://www.cisa.gov/sites/default/files/2024-05/FY%202024%20IG%20FISMA%20Metrics%20Evaluation%20Guide%20Final.pdf.

Appendix V
Report Distribution

Federal Labor Relations Authority

Colleen Duffy Kiko, Member
Anne M. Wagner, Member
Michael Jeffries, Executive Director
Dave Fontaine, Chief Information Officer
Thomas Tso, 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-FILE_A_COMPLAINT

EMAIL: OIGMAIL@FLRA.GOV
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 2024