UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Memorandum

August 16, 2024

To: Prem Aburvasamy
Chief Information Officer

From: Kevin N. Thomas KEVIN THOMAS Digitally signed by KEVIN THOMAS Date: 2024.08.16 09:53:46 -04'00'
Acting Inspector General

Subject: FY 2024 FISMA
(OIG-AMR-106-24-04)

This memorandum transmits the audit report "National Labor Relations Board (NLRB) Federal Information Security Modernization Act Audit for Fiscal Year 2024" with the Management Response.

We contracted with Castro & Company, an independent public accounting firm, to audit the NLRB's compliance with Federal Information Security Modernization Act (FISMA). The contract required that the audit be done in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

In connection with the contract, we reviewed Castro & Company's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, a conclusion about the NLRB's compliance with FISMA. Castro & Company is responsible for the attached auditor's report dated August 15, 2024, and the conclusions expressed in the report. Our review disclosed no instances where Castro & Company did not comply, in all material respects, with generally accepted government auditing standards.

We request that the OCIO provide an Action Plan to implement the audit's recommendation. Action Plans should be provided to the OIG and the Audit Follow-up Official within 30 days of the issuance the audit report. For this audit, the Chief of Staff is the Audit Follow-up Official.

We appreciate the courtesies and cooperation extended to Castro & Company and our staff during the audit.

cc: Board
General Counsel
Audit Follow-up Official/Chief of Staff

National Labor Relations Board (NLRB)
Federal Information Security Modernization Act Audit
for Fiscal Year 2024

August 15, 2024

Submitted By:

Castro & Company, LLC
1635 King Street
Alexandria, VA 22314
Phone: (703) 229-4440
Fax: (703) 859-7603

Table of Contents

I. EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (FISMA) requires the National Labor Relations Board (NLRB or Agency) to develop, document, and implement an agency wide security program for the information and the information systems that support the operations and assets of the Agency. FISMA also requires that each Inspector General perform an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. Castro & Company, LLC (Castro & Co) was contracted by the NLRB's Inspector General to perform the Agency's Fiscal Year (FY) 2024 FISMA audit.

Our objective was to evaluate the effectiveness of the NLRB's security program and practices. Specifically, we reviewed the status of the NLRB's Information Technology (IT) security program in accordance with the FY 2023 – 2024 Inspector General FISMA Reporting Metrics (published on February 10, 2023). The FY 2023 – 2024 Inspector General FISMA metrics focused on 20 core metrics and 17 FY 2024 supplemental metrics. These metrics consisted of five security functions aligned with nine metric domains:

1. Identify (Two Domains: Risk Management, Supply Chain Risk Management);
2. Protect (Four Domains: Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training);
3. Detect (One Domain: Information Security Continuous Monitoring);
4. Respond (One Domain: Incident Response); and
5. Recover (One Domain: Contingency Planning).

Using the FY 2024 Inspector General FISMA Metrics, Inspectors General assess the effectiveness of each security function using maturity level scoring prepared by the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The scoring distribution is based on five maturity levels outlined in the FY 2024 Inspector General FISMA Metrics as follows: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. For a security function to be considered "effective", agencies' security programs must score at Managed and Measurable or Optimized.

We determined that the Agency's overall assessed maturity was Optimized with four of the five security functions at the Optimized level and one function at the Managed and Measurable level. Based on the overall maturity level, the NLRB's security program was "effective".

However, we made one recommendation related to Supply Chain Risk Management - Counterfeit Components. The recommendation was provided to the Office of the Chief Information Officer (OCIO) to strengthen and improve NLRB's information security program.

II. BACKGROUND

The Federal Information Security Modernization Act of 2014 requires agencies to develop, document, and implement an agency wide security program for the information and the information systems that support the operations and assets of the agency, including those provided by another agency, a contractor, or another source. FISMA also requires that each Inspector General perform an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency, including testing the effectiveness of information security policies, procedures, and practices for select systems.

To support the annual independent evaluation requirements, OMB, DHS, and CIGIE developed annual FISMA reporting metrics for Inspectors General to answer. This guidance directs Inspectors General to evaluate the effectiveness of agency information security programs across a variety of attributes grouped into nine security domains: risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning. Each domain is rated on a maturity level spectrum ranging from "Ad Hoc" to "Optimized". The maturity level definitions for the Inspector General FISMA reporting metrics are:

- Level 1 (Ad Hoc) – Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
- Level 2 (Defined) – Policies, procedures, and strategies are formalized and documented but not consistently implemented.
- Level 3 (Consistently Implemented) – Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
- Level 4 (Managed and Measurable) – Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
- Level 5 (Optimized) – Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

III. OBJECTIVE, SCOPE AND METHODOLOGY

Our objective was to perform an independent audit of the effectiveness of the NLRB's information security program and practices. In support of this objective, we prepared responses to the annual Inspector General FISMA reporting metrics, which the NLRB's OIG submitted via the DHS automated application (CyberScope) in accordance with OMB guidance. The scope of the audit was to assess the maturity level of the NLRB's IT Security program as of the end of fieldwork for FY 2024. We performed this audit from May through July 2024 by obtaining evidence primarily from OCIO stakeholders from NLRB's Headquarters located in Washington, D.C. to comply with the CyberScope reporting deadlines within the FY 2024 Inspector General FISMA Reporting Metrics. This review period was from October 1, 2023 through March 31, 2024.

Based on the requirements specified in FISMA and the FY 2024 Inspector General FISMA Reporting Metrics, our audit focused on reviewing the five security functions and nine associated metric domains: Identify (Two Domains: Risk Management, Supply Chain Risk Management), Protect (Four Domains: Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training), Detect (One Domain: Information Security Continuous Monitoring), Respond (One Domain: Incident Response), and Recover (One Domain: Contingency Planning).

For the ratings, we used a calculated average approach, wherein the average of the metrics in a particular domain were used to determine the effectiveness of individual function areas (Identify, Protect, Detect, Respond, and Recover) and the overall information security program. As part of this approach, Core metrics and Supplemental metrics were averaged independently to determine

a domain's maturity calculation and provide data points for the assessed program and function effectiveness. In determining maturity levels and the overall effectiveness of the agency's information security program, we focused on the results of the Core metrics and used the calculated averages of the Supplemental metrics to support our determination of the overall program and function level effectiveness.

We obtained and reviewed NLRB's policies and procedures, as well as Governmentwide guidance relating to IT Security, including from OMB and the National Institute of Standards and Technology (NIST). We interviewed staff in the OCIO with IT Security roles to gain an understanding of the Agency's system security and application of management, operational, and technical controls. We obtained documentation related to the application of those controls. We then reviewed the documentation provided to address the specific reporting metrics outlined in the FY 2024 Inspector General FISMA reporting metrics.

Tests procedures were performed to evaluate the NLRB security program to provide reasonable assurance that the controls tested were operating effectively throughout the period under audit. To determine a control sample size, we considered the size of the population and leveraged GAO and CIGIE's Financial Audit Manual 360.07 and 460.02 as general guidance for the sampling approach. When planning sampling control testing, we determined a sample size sufficient to reduce sampling risk to an acceptably low level (AU-C 530.07). Our sampling approach documented the objectives of the test, population (including sampling unit and time frame), method of selecting sample, and sample design and resulting sample size.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence (such as NLRB policies and procedures, system security plans, plan of actions and milestones, system reporting/dashboards, and system configurations) 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.

IV. SUMMARY OF RESULTS

Based on the FY 2024 Inspector General FISMA metrics requirements, our testing concluded that NLRB has implemented an "effective" information security program for FY 2024. In comparison with the FY 2023 FISMA submission, the maturity levels for FY 2024 are as follows:

Function	Domain	Assessment in CyberScope 2023	Assessment in CyberScope 2024
1: Identify	Risk Management / Supply Chain Risk Management	Managed and Measurable	Managed and Measurable
2: Protect	Configuration Management / Identity and Access Management / Data Protection & Privacy / Security Training	Optimized	Optimized
3: Detect	Information Security Continuous Monitoring	Optimized	Optimized
4: Respond	Incident Response	Optimized	Optimized
5: Recover	Contingency Planning	Optimized	Optimized

V. FINDING

Castro & Co identified one deficiency in the general IT control area of Supply Chain Risk Management, specifically related to the Counterfeit Components. During our review, we noted the following:

1. Component Authenticity/Anticounterfeit Training

Based on testing performed and evidence reviewed, we noted authenticity/anti-counterfeit training to detect counterfeit system components (including hardware, software, and firmware) was not provided to designated personnel as required by the NIST Special Publication (SP) 800-53 Revision 5, Component Authenticity, Anti-Counterfeit Training (SR-11[1]).

In FY 2024, NLRB provided Supply Chain Risk Management training to Contracting Officers; however, the training did not include specific modules related to counterfeit detection.

Without authenticity/anti-counterfeit training for designated personnel and roles, there is an increased risk of counterfeit components entering the organization's system(s) and introducing malicious code.

VI. RECOMMENDATION

We recommend that the designated personnel complete training in detecting counterfeit system components (including hardware, software, and firmware) and best practices for counterfeit component prevention.

VII. APPENDIX A – Management's Response

National Labor Relations Board (NLRB)
Federal Information Security Modernization Act Audit
For Fiscal Year 2024

UNITED STATES GOVERNMENT

National Labor Relations Board
Office of the Chief Information Officer

Memorandum

To: Kevin Thomas
Acting Inspector General

From: Prem Aburvasamy
Chief Information Officer

Date: August 14, 2024

Subject: OIG FISMA Audit Report – OIG-AMR-106

Management Response:

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report, 2024 Federal Information Security Modernization Act (FISMA) Audit for the National Labor Relation Board (NLRB), Report OIG-AMR-106. The OIG audits are always valuable as they afford us an independent assessment of our operations and help inform our continuous efforts to enhance the security of our program. OCIO concurs with the recommendation and will be performing corrective actions to ensure that the designated personnel are trained for Counterfeit Detection as required by the NIST SP 800-53 rev5, Component Authenticity, Anti-Counterfeit Training (SR-11[1]).

OCIO has received an overall rating of "Effective" this year. The rating was the direct result of sufficient budget funding, resources, and the support of Agency Leadership.

I appreciate the opportunity to respond to the draft report. If you have any questions or need additional information regarding our response, please contact me.