UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Memorandum

August 26, 2022

To: Prem Aburvasamy
Chief Information Officer

From: David P. Berry
Inspector General

Subject: FY 2022 FISMA
(OIG-AMR-100)

This memorandum transmits the audit report "National Labor Relations Board (NLRB) Federal Information Security Modernization Act Audit for Fiscal Year 2022" with the Management Response.

We contracted with Castro & Company, an independent public accounting firm, to audit the NLRB's compliance with 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 26, 2022, 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 Office of the Chief Information Officer provide an Action Plan to implement the audit's recommendation. Action Plans should be provided to the Office of Inspector General 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 2022

August 26, 2022

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) 2022 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 security program in accordance with the FY 2022 Inspector General FISMA Reporting Metrics. The FY 2022 Inspector General FISMA metrics focused on 20 core 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 2022 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 2022 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 or above Managed and Measurable.

We determined that the Agency's overall assessment rating was "effective" with all five security functions at the Optimized level. This marks an improvement from the prior year's rating where the Agency had two security functions at the Managed and Measurable level and three functions at the Optimized level.

However, we made one recommendation specifically regarding the Agency's System Security and Privacy Plans. 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 FY 2022 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 Agency's Information Technology (IT) Security program as of the end of fieldwork for FY 2022. We performed this audit from April through July 2022. Because the FY 2022 Inspector General FISMA Reporting Metrics contained a new accelerated deadline, this review period was from October 1, 2021 through March 31, 2022.

Based on the requirements specified in FISMA and the FY 2022 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).

Ratings throughout the nine domains were calculated by simple majority, where the most frequent level (i.e., the mode) across the questions will serve as the domain rating. The domain ratings were used to determine the overall function ratings. The function ratings were then used to determine the overall Agency rating.

We obtained and reviewed Governmentwide guidance relating to IT Security, including from OMB and the National Institute of Standards and Technology (NIST). We obtained and reviewed the Agency's policies and procedures related to IT Security. 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 2022 Inspector General FISMA reporting metrics.

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 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 2022 Inspector General FISMA metrics requirements, our testing concluded that NLRB has implemented an "effective" information security program for FY 2022. NLRB continued to improve its information security program and made progress in implementing all recommendations resulting from previous FISMA evaluations. In comparison with the FY 2021 FISMA submission, the maturity levels increased as follows:

Function	Domain	Ranking Assigned in CyberScope 2021	Ranking Assigned in CyberScope 2022
1: Identify	Risk Management / Supply Chain Risk Management	Optimized	Optimized
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	Managed and Measurable	Optimized
5: Recover	Contingency Planning	Managed and Measurable	Optimized

V. FINDINGS

Castro & Co identified one deficiency in the general IT control area of Information Security Continuous Monitoring, specifically related to the System Security and Privacy Plan. During our review, we noted the following:

1. System Security and Privacy Plan

During our audit procedures, we noted a System Security Plan was last updated in October 2018 and had not been updated to reflect the latest controls as required by the NIST Special Publication (SP) 800-53 Revision 5, System Security and Privacy Plans (PL-2).

According to the OCIO, due to budget constraints and resource issues, the OCIO did not update the System Security and Privacy Plan (previously referred to as System Security Plan) to reflect the latest controls in NIST SP 800-53 Revision 5. The OCIO stated that they will be incorporating the updates in FY 2023.

By not updating the System Security and Privacy Plan to incorporate the latest controls in NIST SP 800-53 Revision 5, the system's security and protection could be at risk of being exploited.

VI. RECOMMENDATION

We recommend that the OCIO perform corrective actions to ensure that the System Security and Privacy Plan is updated to comply with NIST 800-53 Revision 5.

VII. APPENDIX A – Management's Response

UNITED STATES GOVERNMENT
National Labor Relations Board
Office of the Chief Information Officer

Memorandum

To: David Berry Inspector General

From: Prem Aburvasamy
Chief Information Officer

Date: August 25, 2022

Subject: OIG FISMA Audit Report – OIG-AMR-100

Management Response:

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report, 2022 FISMA Information Security Modernization Act (FISMA) Audit for the National Labor Relation Board (NLRB), Report OIG-AMR-100. 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 the System Security and Privacy Plan is updated to comply with NIST 800-53 Revision 5.

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.