National Labor Relations Board (NLRB)
Federal Information Security Modernization Act Audit
for Fiscal Year 2021

November 22, 2021

Submitted By:

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

Table of Contents

National Labor Relations Board (NLRB)
Federal Information Security Modernization Act Audit
For Fiscal Year 2021

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 was contracted by the NLRB's Inspector General to perform the Agency's Fiscal Year 2021 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 Fiscal Year 2021 Inspector General FISMA Reporting Metrics. These metrics consisted of five security functions aligned with nine 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).

Using the Fiscal Year 2021 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, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency. The scoring distribution is based on five maturity levels outlined in the Fiscal Year 2021 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 two of the five security functions at the Managed and Measurable level and the remaining three at the Optimized level. This marks an improvement from the prior years rating that had two security functions at the Optimized level.

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, the Office of Management and Budget (OMB), the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency 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 Fiscal Year (FY) 2021 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 evaluate the effectiveness of the NLRB's information security program and practices. The scope of the audit was the status of the maturity level of the Agency's Information Technology (IT) Security program as of the end of fieldwork for FY 2021.

Based on the requirements specified in FISMA and the FY 2021 Inspector General FISMA 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 Office of the Chief Information Officer (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 2021 Inspector General FISMA reporting metrics.

We conducted this performance audit in accordance with generally accepted government auditing standards during the period from May 24, 2021 through September 30, 2021. 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

During FY 2021, the NLRB's OCIO made improvements in its IT Security posture. In comparison with the FY 2020 FISMA submission, the maturity level increased as follows:

Identify Function

Risk Management

Function 1A: Identify – Risk Management		
	2020	**2021**
Functional Rating	**Optimized**	**Optimized**

Supply Chain Risk Management[1]

Function 1B: Identify – Supply Chain Risk Management		
	2020	**2021**
Functional Rating	**Not Tested**	**Defined**

[1] The Supply Chain Risk Management requirements became effective on September 24, 2021, and are not included in the overall assessment rating.

Protect Function

Configuration Management

Function 2A: Protect – Configuration Management		
	2020	2021
Functional Rating	Managed and Measureable	Managed and Measureable

Identity and Access Management

Function 2B: Protect – Identity and Access Management		
	2020	2021
Functional Rating	Optimized	Optimized

Data Protection and Privacy

Function 2C: Protect – Data Protection and Privacy		
	2020	2021
Functional Rating	Optimized	Optimized

Security Training

Function 2D: Protect – Security Training		
	2020	2021
Functional Rating	Optimized	Optimized

Detect Function *– Information Security Continuous Monitoring (ISCM)*

Function 3: Detect – ISCM		
	2020	2021
Functional Rating	Managed and Measureable	Optimized

Respond Function *- Incident Response*

Function 4: Respond – Incident Response		
	2020	2021
Functional Rating	Managed and Measureable	Managed and Measureable

Recover Function *- Contingency Planning*

Function 5: Recover – Contingency Planning		
	2020	2021
Functional Rating	Managed and Measureable	Managed and Measureable

V. FINDINGS

Based upon the FY 2021 Inspector General metrics, our testing did not identify deficiencies with respect to the effectiveness of the NLRB's security program and practices, and the NLRB received an overall rating of "effective."

VI. 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: November 22, 2021

Subject: OIG FISMA Audit Report – OIG-AMR-96

Management Response:

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report, 2021 FISMA Information Security Modernization Act (FISMA) Audit for the National Labor Relation Board (NLRB), Report (OIG-AMR-96). The OIG comments are valuable as they afford us an independent assessment of our operations and help inform our continuous efforts to enhance the security of our program. During FY 21 the Office of the Chief Information Officer (OCIO) closed the one recommendation from the FY 20 OIG FISMA Audit. To achieve compliance with the President's Executive Order on Improving the Nation's Cybersecurity (14028), the OCIO will continue to develop and implement its supply chain management program and insider threat program over the course of FY 22 within our funding and resources.

OCIO has received an overall rating of "Effective" for the second year was only possible because of the budget, resource, 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.