UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Memorandum

November 17, 2020

To: Prem Aburvasamy
Chief Information Officer

From: David P. Berry
Inspector General

Subject: FY 2020 FISMA
(OIG-AMR-93-21-02)

This memorandum transmits the audit report "National Labor Relations Board (NLRB) Federal Information Security Modernization Act Audit for Fiscal Year 2020" 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 November 17, 2020, 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 2020

November 17, 2020

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 2020

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 2020 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 2020 Inspector General FISMA Reporting Metrics. These metrics consisted of five security functions aligned with eight metric domains:

- Identify (One Domain: 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).

Under the Fiscal Year 2020 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 2020 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 has made improvements in all five security functions, as this year three of the five were at Managed and Measurable and two of the five were Optimized. As a result, the overall assessment of NLRB's information security program is effective.

II. BACKGROUND

The Federal Information Security Modernization Act of 2014 (FISMA) 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 (IG) 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 eight security domains: 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) 2020 IG 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 2020.

Based on the requirements specified in FISMA and the FY 2020 IG FISMA Metrics, our audit focused on reviewing the five security functions and eight associated metric domains: Identify (One Domain: 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 eight 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 2020 IG FISMA reporting metrics.

We conducted this performance audit in accordance with generally accepted government auditing standards during the period May 21, 2020 through September 30, 2020. 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 2020, the NLRB's OCIO made improvements in its IT Security posture. In comparison with the FY 2019 FISMA submission, the maturity level increased as follows:

Identify – *Risk Management*

Function 1: Identify – Risk Management		
	2019	**2020**
Ad Hoc	1	0
Defined	1	1
Consistently Implemented	9	0
Managed and Measurable	1	5
Optimized	0	6
Functional Rating	**Consistently Implemented**	**Optimized**

Protect

Configuration Management

Function 2A: Protect – Configuration Management		
	2019	**2020**
Ad Hoc	0	0
Defined	0	0
Consistently Implemented	3	0
Managed and Measurable	5	8
Optimized	0	0
Functional Rating	**Managed and Measureable**	**Managed and Measureable**

Identity and Access Management

Function 2B: Protect – Identity and Access Management		
	2019	**2020**
Ad Hoc	1	0
Defined	3	0
Consistently Implemented	4	0
Managed and Measurable	1	3
Optimized	0	6
Functional Rating	**Consistently Implemented**	**Optimized**

Data Protection and Privacy

Function 2C: Protect – Data Protection and Privacy		
	2019	**2020**
Ad Hoc	1	0
Defined	1	0
Consistently Implemented	3	0
Managed and Measurable	0	0
Optimized	0	5
Functional Rating	**Consistently Implemented**	**Optimized**

Security Training

Function 2D: Protect – Security Training		
	2019	**2020**
Ad Hoc	0	0
Defined	0	0
Consistently Implemented	0	0
Managed and Measurable	6	1
Optimized	0	5
Functional Rating	**Managed and Measureable**	**Optimized**

Detect *– Information Security Continuous Monitoring (ISCM)*

Function 3: Detect – ISCM		
	2019	**2020**
Ad Hoc	0	0
Defined	0	0
Consistently Implemented	5	0
Managed and Measurable	0	3
Optimized	0	2
Functional Rating	**Consistently Implemented**	**Managed and Measureable**

Respond *- Incident Response*

Function 4: Respond – Incident Response		
	2019	**2020**
Ad Hoc	0	0
Defined	0	0
Consistently Implemented	5	2
Managed and Measurable	2	3
Optimized	0	2
Functional Rating	**Consistently Implemented**	**Managed and Measureable**

Recover *- Contingency Planning*

Function 5: Recover – Contingency Planning		
	2019	**2020**
Ad Hoc	0	0
Defined	1	0
Consistently Implemented	6	2
Managed and Measurable	0	3
Optimized	0	2
Functional Rating	**Consistently Implemented**	**Managed and Measureable**

V. FINDINGS

Our testing identified a deficiency in one general IT control subject area: System and Services Acquisition. During our review, we noted the following issue:

1. Acquisition Policy

During our audit procedures, we noted the following:

The NIST guidance provides for the establishment of requirements, descriptions, and criteria that should be contained within acquisition contracts for the information system, system component, or information system service to ensure that agency data is adhering to standards that meet or exceed the NIST requirements. These requirements, descriptions, and criteria should be included within the Acquisition policy to ensure that contracts contain the necessary language so that external service providers adhere to the same or more stringent security requirements as the NLRB.

Upon review of the Acquisition policy, it was determined that there were no references relating to the following:

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Description of the information system development environment and environment in which the system is intended to operate; and
f. Acceptance criteria.

The following criteria relates to the condition identified above:

- NIST Special Publication (SP) 800-53, Revision 4, System and Services Acquisition Policy and Procedures (SA-1)
- NIST SP 800-53, Revision 4, Acquisition Process (SA-4)

Without specific requirements, descriptions, and criteria in the Acquisition policy, there is the risk that the NLRB will enter into acquisition contracts where data will not be protected in accordance with NIST or at least meet the minimum standards within NIST.

VI. RECOMMENDATIONS

We recommend that the OCIO:

1. Ensure the Acquisition policy is updated to reflect the requirements and criteria contained within SA-4 from NIST SP 800-53 Revision 4.

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 12, 2020
Subject:	OIG FISMA Audit Report – OIG-AMR-93

Management Response:

Recommendation:

1. Ensure the Acquisition Policy is updated to reflect the requirements and criteria contained withing SA-4 from NIST SP 800-53 Revision 4.

OCIO concurs with the FISMA 2020 report and recommendation. OCIO will work with the Office of Acquisition to revise the Agency Acquisition Policy as identified in NIST SP 800-53 R4 (SA-4) with the necessary language to ensure external service providers adhere to Agency IT security requirements.