UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Federal Information Security Modernization Act Audit
Fiscal Year 2018

Report No. OIG-AMR-87-19-02

July 12, 2019

CONTENTS

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.

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 2018 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 2018 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 2018 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 can make improvements in all five security functions, as none of the five were at Managed and Measurable. We made one recommendation for corrective action.

The Management Comments state that the Office of the Chief Information Officer concurs with the content of the audit report and acknowledges the recommendations. The Management Comments also request that the Office of Inspector General make a correction to its Fiscal Year 2018 CyberScope FISMA template. As discussed in the body of the audit report, we determined that the

suggested correction would be inappropriate. The Management Comments are included in their entirety as an appendix to the report.

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 (DHS), 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" for not having formalized policies, procedures, and strategies, to "Optimized" for having policies, procedures, and strategies that are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

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 Fiscal Year (FY) 2018.

Based on the requirements specified in FISMA and the FY 2018 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. 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 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 2018 IG FISMA reporting metrics.

We conducted this performance audit in accordance with generally accepted government auditing standards during the period April 2018 through October 2018. 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.

FINDINGS

During FY 2018, the NLRB's Office of the Chief Information Officer made improvements in its Information Technology

posture. In comparison with the FY 2017 FISMA submission, which we did not complete as an audit, the maturity level increased in 26 (48 percent) of the 54 metric domains from 2017. Of those 26:

- Two increased from the targeted maturity level – Managed and Measurable to the maximum maturity level, Optimized;
- One increased from Consistently Implemented to the targeted maturity level – Managed and Measurable;
- Two increased from Defined to Consistently Implemented;
- Ten increased two maturity levels from Ad Hoc to Consistently Implemented; and
- Eleven increased from Ad Hoc to Defined.

We also identified, however, that all five of the security function areas fell short of meeting the targeted Managed and Measurable maturity level for effectiveness.

Identify – Risk Management

The Identify security function is comprised of the Risk Management metric domain. Based on our evaluation, the calculated maturity level for the Identify/Risk Management security function/metric domain was at Ad Hoc, which is categorized as being not effective.

This domain consists of the following metric categories: Information System Inventory; Inventory of Hardware Assets; Inventory of Software and Associated Licenses; Categorization of Information Systems; Risk Management Policies, Procedures, and Strategy; Information Security Architecture; Roles and Responsibilities of the Risk Management Stakeholders; Plans of Action and Milestones; Policies and Procedures – Risk Assessment; Communication of Risks; Contracting Language and Service Level Agreements; and Portfolio View of the Risk.

Of the twelve metrics in this domain, we found that one was at Consistently Implemented; four were at Defined; and seven were at Ad Hoc.

Protect

The Protect security function is comprised of the following metric domains: Configuration Management; Identity and Access Management; Data Protection and Privacy; and Security Training. Based on our evaluation, the calculated maturity level for the Protect security function was at Consistently Implemented, which is categorized as being not effective.

Configuration Management

Based on our evaluation, the calculated maturity level for the Configuration Management (CM) domain was at Consistently Implemented.

This domain consists of the following metric categories: Roles and Responsibilities of the CM Stakeholders; Enterprise Wide CM Plan; CM Policies & Procedures Defined; Standard Baseline Configurations; Configuration Settings/Common Secure Configurations; Flaw Remediation Processes; Trusted Internet Connection; and Configuration Change Control Processes.

Of the eight metrics in this domain, we found that four were at Consistently Implemented; two were at Defined; and two were at Ad Hoc.

Identity and Access Management

Based on our evaluation, the calculated maturity level for the Identity and Access Management domain was at Defined.

This domain consists of the following metric categories: Roles and Responsibilities of Identity, Credential, and Access Management (ICAM) stakeholders; ICAM Strategy; ICAM Policies and Procedures; Assessing Personnel Risk Designations and Screening; Access Agreements; Personal Identity Verification (PIV)/Level of Assurance (LOA) Credential – Non Privileged Users; PIV/LOA – Privileged Users; Tracking/Controlling use of Privileged Accounts; and Ensure Configuration/Connection Requirements are Maintained.

Of the nine metrics in this domain, we found that two were at Optimized; one was at Consistently Implemented; four were at Defined; and two were at Ad Hoc.

Data Protection and Privacy

Based on our evaluation, the calculated maturity level for the Data Protection and Privacy domain was at Consistently Implemented.

This domain consists of the following metric categories: Privacy Program for Protection of Personally Identifiable Information (PII); Security Controls over PII and Sensitive Data; Data Exfiltration -– Enhance Network Defenses; Data Breach Response Plan; and Privacy Awareness Training.

Of the five metrics in this domain, we found that two were at Consistently Implemented; one was at Defined; and two were at Ad Hoc.

Security Training

Based on our evaluation, the calculated maturity level for the Security Training domain was at Consistently Implemented.

This domain consists of the following metric categories: Roles and Responsibilities of the Security Awareness and Training (SAT) Stakeholders; Assessment of Skills, Knowledge, and Abilities; Defined SAT Program Strategy/Plan; Security Training Policy/Procedures; Identification/Tracking SAT; and Training – Significant IT Responsibilities.

Of the six metrics in this domain, we found that two were at Consistently Implemented; two were at Defined; and two were at Ad Hoc.

Management Comments

The Management Comments state:

> The OIG Audit Report rates the OCIO as "Consistently Implemented" for Protect category function. The OIG rated the OCIO as Defined for Protection in the FY2018 CyberScope submission. The OCIO requests updating of the CyberScope submission to reflect the

"Consistently Implemented" rating for CyberScope Function 2.

OIG Response

In the OIG FISMA CyberScope template, there are two Maturity Levels by Function – "Calculated Maturity Level" and "Assessed Maturity Level." For Function 2: Protect, we reported the Calculated Maturity Level as "Consistently Implemented" and the Assessed Maturity Level as "Defined." For purposes of the audit report, we used the Calculated Maturity Level as clearly identified in the draft audit report. We used the Calculated Maturity Level because we viewed it as less subjective than the Assessed Maturity Level and it is consistent with what we observed in the Inspector General community. As such, we determined that there is no need to make the OCIO's suggested correction.

Detect – Information Security Continuous Monitoring

The Detect security function is comprised of the Information Security Continuous Monitoring metric domain. Based on our evaluation, the calculated maturity level for the Detect/Information Security Continuous Monitoring security function/metric domain was at Defined, which is categorized as being not effective.

This domain consists of the following metric categories: Information Security Continuous Monitoring (ISCM) strategy; ISCM Processes Defined; ISCM Stakeholders; Processes for Ongoing Authorizations; and Performance Measures.

Of the five metrics in this domain, we found that four were at Defined; and one was at Ad Hoc.

Respond – Incident Response

The Respond security function is comprised of the Incident Response metric domain. Based on our evaluation, the calculated maturity level for the Respond/Incident Response security function/metric domain was at Consistently Implemented, which is categorized as being not effective.

This domain consists of the following metric categories: Incident Response Processes Defined; Incident Response Team Roles; Incident Detection and Analysis; Incident

Handling Process; Sharing Information; Collaboration with DHS/Other Parties; and Incident Response Technologies Defined.

Of the seven metrics in this domain, we found that one was at Managed and Measurable; three were at Consistently Implemented; two were at Defined; and one was at Ad Hoc.

Recover – Contingency Planning

The Recover security function is comprised of the Contingency Planning metric domain. Based on our evaluation, the calculated maturity level for the Recover/Contingency Planning security function/metric domain was at Consistently Implemented, which is categorized as being not effective.

This domain consists of the following metric categories: Roles and Responsibilities of Contingency Planning Stakeholders; Documentation of Contingency Plans; Business Impact Analysis; Development of Contingency Plans; Testing of System Contingency Plans; Backup, Storage, and Alternate Processing Sites; and Planning and Recovering Activities.

Of the seven metrics in this domain, we found that six were at Consistently Implemented; and one was at Ad Hoc.

RECOMMENDATION

We recommend that the Office of the Chief Information Officer perform corrective actions to achieve a Managed and Measurable maturity level for each of the security functions. Specifically, we recommend that the Office of the Chief Information Officer:

1. Prioritize corrective action based on an assessment of the Agency's security risk;

2. Based on that priority, work to remediate the Ad Hoc and Defined metrics to Consistently Implemented; and

3. Implement quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies so the Agency can meet the targeted Managed and Measurable maturity level for its overall security program.

APPENDIX

UNITED STATES GOVERNMENT
National Labor Relations Board

Date: July 8, 2019

To: Robert Brennan, Lead Auditor

From: Prem Aburvasamy, Chief Information Officer

Subject: Response to Federal Information Security Modernization Act Audit – Fiscal Year 2018

The Office of Chief Information Officer (OCIO) reviewed the Draft FISMA audit report and below is the response.

The OCIO concurs with the content of draft FISMA audit report and acknowledges the recommendations.

The OCIO notes the OIG's FY 18 FISMA CyberScope response does not align with the audit report. Specifically:

The OIG Audit Report rates the OCIO as "Consistently Implemented" for Protect category function. The OIG rated the OCIO as Defined for Protection in the FY2018 CyberScope submission. The OCIO requests updating of the CyberScope submission to reflect the "Consistently Implemented" rating for CyberScope Function 2.