UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Memorandum

December 5, 2019

To: Prem Aburvasamy
Chief Information Officer

From: David P. Berry
Inspector General

Subject: Fiscal Year 2019 FISMA
(OIG-AMR-90-20-02)

This memorandum transmits the Independent Evaluation of the National Labor Relations Board (NLRB) Implementation of the Federal Information Security Modernization Act for Fiscal Year 2019 with the Management Response and Auditor's 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 December 5, 2019, 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 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

Independent Evaluation of the National Labor Relations Board (NLRB) Implementation of the Federal Information Security Modernization Act for Fiscal Year 2019

December 5, 2019

Submitted By:

Castro & Company, LLC
1737 King Street Suite 250
Alexandria, VA 22314
Phone: (703) 229-4440
Fax: (703) 859-7603

Table of Contents

National Labor Relations Board (NLRB)
Federal Information Security Modernization Act of 2014
For Fiscal Year 2019

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 2019 FISMA independent evaluation.

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 2019 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 2019 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 2019 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 only one of the five were at Managed and Measurable.

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" 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.

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 Fiscal Year (FY) 2019.

Based on the requirements specified in FISMA and the FY 2019 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 2019 IG FISMA reporting metrics.

We conducted this performance audit in accordance with generally accepted government auditing standards during the period July 9, 2019 through October 30, 2019. 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 2019, the NLRB's Office of the Chief Information Officer made improvements in its Information Technology posture. In comparison with the FY 2018 FISMA submission, the maturity level increased as follows:

***Identify** – Risk Management*

Function 1: Identify – Risk Management		
	2018	**2019**
Ad Hoc	7	1
Defined	4	1
Consistently Implemented	1	9
Managed and Measurable	0	1
Optimized	0	0
Functional Rating	**Ad Hoc**	**Consistently Implemented**

Protect

Configuration Management

Function 2A: Protect – Configuration Management		
	2018	**2019**
Ad Hoc	2	0
Defined	2	0
Consistently Implemented	4	3
Managed and Measurable	0	5
Optimized	0	0
Functional Rating	**Consistently Implemented**	**Managed and Measurable**

Identity and Access Management

Function 2B: Protect – Identity and Access Management		
	2018	**2019**
Ad Hoc	2	1
Defined	4	3
Consistently Implemented	1	4
Managed and Measurable	0	1
Optimized	2	0
Functional Rating	**Defined**	**Consistently Implemented**

Data Protection and Privacy

Function 2C: Protect – Data Protection and Privacy		
	2018	**2019**
Ad Hoc	2	1
Defined	1	1
Consistently Implemented	2	3
Managed and Measurable	0	0
Optimized	0	0
Functional Rating	**Consistently Implemented**	**Consistently Implemented**

Security Training

Function 2D: Protect – Security Training		
	2018	**2019**
Ad Hoc	2	0
Defined	2	0
Consistently Implemented	2	0
Managed and Measurable	0	6
Optimized	0	0
Functional Rating	**Consistently Implemented**	**Managed and Measurable**

Detect *– Information Security Continuous Monitoring (ISCM)*

Function 3: Detect – ISCM		
	2018	**2019**
Ad Hoc	1	0
Defined	4	0
Consistently Implemented	0	5
Managed and Measurable	0	0
Optimized	0	0
Functional Rating	**Defined**	**Consistently Implemented**

***Respond** - Incident Response*

Function 4: Respond – Incident Response		
	2018	**2019**
Ad Hoc	1	0
Defined	2	0
Consistently Implemented	3	5
Managed and Measurable	1	2
Optimized	0	0
Functional Rating	**Consistently Implemented**	**Consistently Implemented**

***Recover** - Contingency Planning*

Function 5: Recover – Contingency Planning		
	2018	**2019**
Ad Hoc	1	0
Defined	0	1
Consistently Implemented	6	6
Managed and Measurable	0	0
Optimized	0	0
Functional Rating	**Consistently Implemented**	**Consistently Implemented**

V. FINDINGS

Our testing identified deficiencies in three general IT control subject areas: system and communications protection, access control, and identification and authentication. During our review, we noted the following issues:

1. Encryption

During our audit procedures, we noted the following:

- Data in transit was not encrypted in accordance with Federal Information Processing Standard (FIPS) 140-2.

The following criteria relates to the condition identified above:

- NIST Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, System and Communications Protection (SC-8)

The Office of the Chief Information Officer did not provide documentation to evidence if the encryption deployed was in accordance with FIPS 140-2.

If data is transmitted in an unencrypted manner, there is the risk that if the data is obtained, the principle of confidentiality will have been violated and thereby expose the agency to privacy and other exposures.

2. Access, Identification and Authentication Policies

During our audit procedures, we noted the following:

- The Access Policy did not contain the necessary details for setting up new users, including procedures for setting up complexity requirements (e.g. password history, password, complexity, etc.).

The following criteria relates to the conditions identified above:

- NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Identification and Authentication (IA-1) and Access Control (AC-1)

The Office of the Chief Information Officer did not follow NIST SP 800-53 Revision 4, last updated January 22, 2015, to adequately document the review and approval of its password policy and document procedures for setting up complexity requirements for new users.

Without reviewing and approving policies timely, there is the risk that the data contained therein will be outdated and IT personnel will be deploying controls that are no longer appropriate.

VI. RECOMMENDATIONS

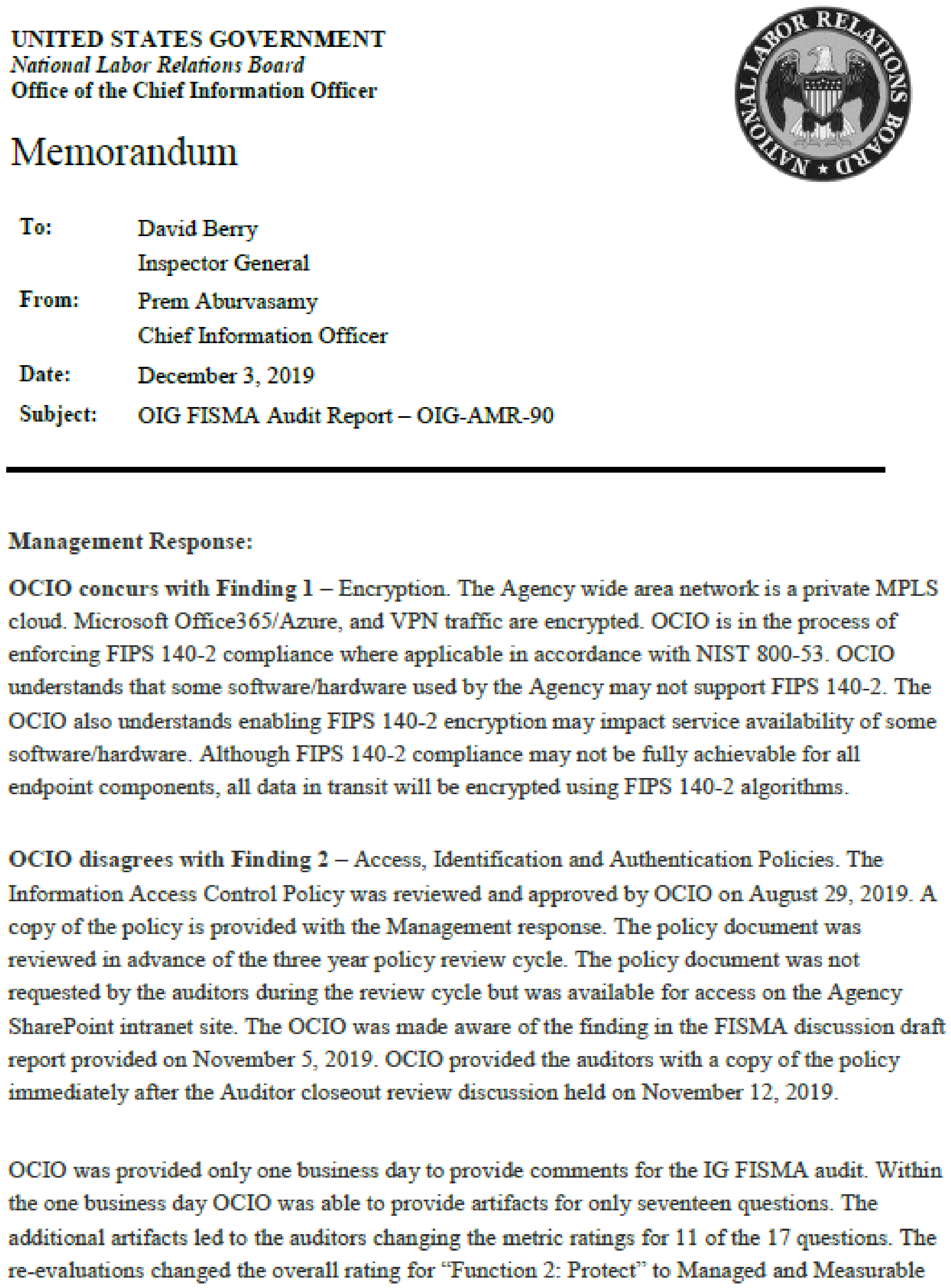
We recommend that the Office of the Chief Information Officer perform corrective actions to achieve a Managed and Measurable maturity level for each of the security functions. Specifically, we recommend that the Office of the Chief Information Officer:

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 A – Management's Response



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

Memorandum

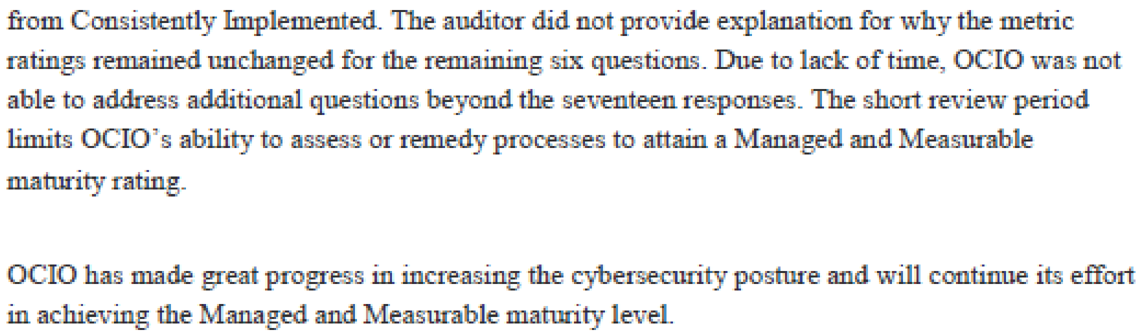
To:	David Berry Inspector General
From:	Prem Aburvasamy Chief Information Officer
Date:	December 3, 2019
Subject:	OIG FISMA Audit Report – OIG-AMR-90

Management Response:

OCIO concurs with Finding 1 – Encryption. The Agency wide area network is a private MPLS cloud. Microsoft Office365/Azure, and VPN traffic are encrypted. OCIO is in the process of enforcing FIPS 140-2 compliance where applicable in accordance with NIST 800-53. OCIO understands that some software/hardware used by the Agency may not support FIPS 140-2. The OCIO also understands enabling FIPS 140-2 encryption may impact service availability of some software/hardware. Although FIPS 140-2 compliance may not be fully achievable for all endpoint components, all data in transit will be encrypted using FIPS 140-2 algorithms.

OCIO disagrees with Finding 2 – Access, Identification and Authentication Policies. The Information Access Control Policy was reviewed and approved by OCIO on August 29, 2019. A copy of the policy is provided with the Management response. The policy document was reviewed in advance of the three year policy review cycle. The policy document was not requested by the auditors during the review cycle but was available for access on the Agency SharePoint intranet site. The OCIO was made aware of the finding in the FISMA discussion draft report provided on November 5, 2019. OCIO provided the auditors with a copy of the policy immediately after the Auditor closeout review discussion held on November 12, 2019.

OCIO was provided only one business day to provide comments for the IG FISMA audit. Within the one business day OCIO was able to provide artifacts for only seventeen questions. The additional artifacts led to the auditors changing the metric ratings for 11 of the 17 questions. The re-evaluations changed the overall rating for "Function 2: Protect" to Managed and Measurable



from Consistently Implemented. The auditor did not provide explanation for why the metric ratings remained unchanged for the remaining six questions. Due to lack of time, OCIO was not able to address additional questions beyond the seventeen responses. The short review period limits OCIO's ability to assess or remedy processes to attain a Managed and Measurable maturity rating.

OCIO has made great progress in increasing the cybersecurity posture and will continue its effort in achieving the Managed and Measurable maturity level.

APPENDIX B – Auditor's Response

The Management's Response in Appendix A states agreement with the findings and recommendation for Finding 1 related to encryption and disagreement with Finding 2 related to the Access, Identification and Authentication Policies.

The basis for the disagreement with Finding 2 is that the OCIO updated the Information Access Control Policy on August 29, 2019, that the policy was updated in advance of the 3-year policy review cycle, that the policy was not requested by the auditors, and that when the OCIO was made aware of the finding it provided the updated policy after the Exit Conference was conducted.

The Management's Response misstates relevant information. On August 13, 2019, the auditors requested documents from the OCIO by providing the OCIO staff with the Provided by Client List (PBC List). In the message transmitting the PBC List, the auditor requested that the OCIO staff member "confirm whether the policy posted in SharePoint is the most current and we can pull from there." The OCIO staff member responded on August 13, 2019 that "[t]he policies and procedures in SharePoint are the most current to date and you can pull from there." The OCIO was aware that the auditor would access the NLRB's policies by obtaining the policies from SharePoint. With that knowledge, it was incumbent upon the OCIO to notify the auditor of any significant changes to policies, particularly in the case of updating a "Dash 1" policy out of cycle. Nevertheless, the OCIO had an access policy that did not meet standards for 11 out of the 12 months of FY 2019 – the scope period under the audit. Given the significant length of time of noncompliance, we determined that it was appropriate for the finding to remain as to report otherwise would be misleading. The policy provided by the OCIO after the Exit Conference was conducted will be reviewed as part of the audit follow-up for FY 2020.

The Management's Response also state that the OCIO was provided with one (1) day to review the draft FISMA matrix and that was not an adequate period of time. Additionally, the Management's Response state that the short period of time to review the draft matrix limited the OCIO's ability to access or remedy processes to attain a "Managed and Measurable" maturity rating because they were not provided information regarding why certain maturity levels were not changed. While we acknowledge that the OCIO was provided with a limited period of time to review the draft FISMA Matrix, potential issues were identified, discussed with and communicated to the OCIO staff in advance of the draft FISMA Matrix being submitted. On September 24, 2019, we met with OCIO staff to discuss documentation that had not yet been provided and, specifically noted during that meeting, that not providing the documentation would result in a finding. Again, on October 9, 2019, we met with the OCIO staff to discuss potential findings on areas that the maturity level appeared to decrease. After the meeting, the OCIO was provided with a list of 34 items for 12 FISMA Matrix questions that would address those potential findings. When the draft FISMA Matrix was provided to the OCIO, each question with a finding below "Managed and Measurable" listed the items needed for the OCIO to meet the next higher maturity; that detailed information was included by the auditors for the benefit of the

OCIO as the auditors are not required to include that information in the FISMA matrix. The final FISMA Matrix also listed, for each question with a finding below "Managed and Measurable," the items that would be necessary to meet the next higher maturity level.

Given the level of specificity that was provided in the draft and final FISMA Matrix, there should be no question for the OCIO on what is needed to attain the "Managed and Measurable" maturity rating. Nevertheless, during the Exit Conference, we explained to the Chief Information Officer that the Department of Homeland Security (DHS) provides a spreadsheet to accompany the FISMA Matrix and the spreadsheet provides detailed information on what is required to meet the various FISMA maturity levels. This spreadsheet is issued by DHS annually in April and is posted to the same DHS Web page as the metrics for Chief Information Officers, Senior Agency Officials for Privacy, and Inspectors General.

The Management's Response appears to shift the responsibility for the FISMA findings from the OCIO to the auditors. As already described, the auditors met with and provided information to the OCIO staff regarding the FISMA findings and the causes. That communication does not and is not intended to shift responsibility for remedial action or future findings to the auditors. It is the CIO's responsibility to review the Government-wide requirements and then implement those requirements through the NLRB's information security internal control environment. Additionally, because the FISMA process is based on a Government-wide matrix that changes in part from year to year, it is the CIO's responsibility to understand and stay updated with the requirements for meeting the "Managed and Measurable" standard independent of any prior audit.