National Labor Relations Board (NLRB)
Federal Information Security Modernization Act Audit
for Fiscal Year 2026

August 19, 2026

Submitted By:

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

UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Memorandum

August 27, 2026

To: Prem Aburvasamy
Chief Information Officer

From: Ruth Blevins
Inspector General

Subject: *Federal Information Security Modernization Act Audit for Fiscal Year 2026*
(OIG-AMR-108-26-01)

This memorandum transmits the audit report *National Labor Relations Board (NLRB) Federal Information Security Modernization Act Audit for Fiscal Year 2026* with the Management Response.

We contracted with Castro & Company, an independent public accounting firm, to audit the NLRB's compliance with the Federal Information Security Modernization Act (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 19, 2026, 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
Chief of Staff

Table of Contents

I. EXECUTIVE SUMMARY 1
II. BACKGROUND 2
III. OBJECTIVE, SCOPE AND METHODOLOGY 3
IV. SUMMARY OF RESULTS 4
V. FINDINGS AND RECOMMENDATIONS 5
VI. APPENDIX A – MANAGEMENT'S RESPONSE 6
VII. APPENDIX B – FISMA OPEN RECOMMENDATIONS 7

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. The NLRB Office of Inspector General contracted with Castro & Company, LLC (Castro & Company) to perform the NLRB's fiscal year (FY) 2026 FISMA performance audit.

For FY 2026, we utilized the *Fiscal Year 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, dated April 3, 2025, required by Office of Management and Budget (OMB) Memorandum M-25-04 ("*FY 2025 Guidance on Federal Information Security and Privacy Management Requirements")* published on January 15, 2025, as mandated by the Cybersecurity and Infrastructure Security Agency (CISA) on May 17, 2026. Therefore, for FY 2026, our evaluation included the same 20 core IG FISMA metrics, as well as five supplemental metrics, assessed in the FY 2025 NLRB FISMA performance 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 (IT) security program in accordance with the Fiscal Year 2025 Inspector General FISMA Reporting Metrics. The FY 2025 Inspector General FISMA Reporting Metrics focused on 20 core metrics and five supplemental metrics. These metrics consisted of six functions aligned with ten domains:

1. Govern (Two Domains: Cybersecurity Governance, Cybersecurity Supply Chain Risk Management (C-SCRM));
2. Identify (One Domain: Risk and Asset Management (RAM));
3. Protect (Four Domains: Configuration Management, Identity and Access Management (IDAM), Data Protection and Privacy, and Security Training);
4. Detect (One Domain: Information Security Continuous Monitoring (ISCM));
5. Respond (One Domain: Incident Response); and
6. Recover (One Domain: Contingency Planning).

Using the FY 2025 Inspector General FISMA Reporting Metrics, auditors assessed the effectiveness of each security function using maturity level scoring prepared by the 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 2025 Inspector General FISMA Reporting Metrics as follows: Ad-Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. For a security function to be considered "effective", an agency's security program must score at Managed and Measurable or Optimized.

We determined that the NLRB's overall assessed maturity was Managed and Measurable with four of the six functions at the Managed and Measurable level and two functions at the Optimized level. Based on the overall assessed maturity, the NLRB's security program was "effective".

We caution that projecting the results of our audit to future periods is subject to the risk that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

This report is intended solely for the information and use of the NLRB, the NLRB Office of Inspector General (OIG), the DHS, OMB, the appropriate committees of Congress, and the Controller General and is not intended for use by anyone other than these specified parties.

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 independent annual 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.

National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (CSF)

The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise, and it provides Inspectors General with guidance for assessing the maturity of controls to address the associated risks. The FY 2025 FISMA Inspector General Reporting Metrics are aligned to the six function areas in the NIST CSF which include Govern, Identify, Protect, Detect, Respond, and Recover.

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 six functions aligned with ten domains:

NIST Cybersecurity Framework Alignment with the IG FISMA Domains Assessed for Fiscal Year 2026	
NIST Cybersecurity Framework Functions	**IG FISMA Domains Assessed for Fiscal Year 2026**
Govern	Cybersecurity Governance Cybersecurity Supply Chain Risk Management
Identify	Risk and Asset Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Inspector General Maturity Levels

OMB and DHS prepared the maturity level scoring. Level 1 (Ad-Hoc) represents the lowest maturity level and Level 5 (Optimized) represents the highest maturity level. For a security function to be considered "effective," agencies' security programs must score at or above Managed and Measurable. The maturity level definitions for the 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 NLRB's IT security program as of the end of fieldwork for FY 2026. Our testing evaluated the General Support System (GSS), as this system provides the critical IT operations for supporting NLRB's mission and daily operations. We performed this audit from May through July 2026 by obtaining evidence primarily from OCIO stakeholders from NLRB's headquarters located in Washington, D.C., to comply with the CyberScope reporting deadlines within the FY 2025 Inspector General FISMA Reporting Metrics. The review period was October 1, 2025 through May 31, 2026.

Based on the requirements specified in FISMA and the FY 2025 Inspector General FISMA Reporting Metrics, our audit focused on reviewing the six functions and ten associated metric domains as stated in the FY 2025 FISMA Inspector General Reporting Metrics.

For the ratings, we used a calculated average approach, wherein the average of the metrics in a particular domain was used to determine the effectiveness of individual function areas (Govern, Identify, Protect, Detect, Respond, and Recover) and the overall information security program. As part of this approach, core metrics and supplemental metrics were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. In determining maturity levels and the overall effectiveness of the agency's information security program, we focused on the results of the core metrics and used the calculated averages of the supplemental metrics to support our determination of the overall program and function-level effectiveness.

We obtained and reviewed NLRB's policies and procedures, as well as government-wide guidance relating to IT security, including from OMB and the National Institute of Standards and Technology (NIST). We interviewed OCIO personnel with IT security roles to gain an understanding of the Agency's system security and application of management, operational, and technical controls. In addition, 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 2025 Inspector General FISMA Reporting Metrics.

Test procedures were performed to evaluate the NLRB security program and to provide reasonable assurance that the controls tested were operating effectively throughout the period under audit. To determine a control sample size, we considered the size of the population and leveraged U.S. Government Accountability Office (GAO) and CIGIE's Financial Audit Manual 460.02 as general guidance for the sampling approach. When planning sampling control testing, we determined a sample size sufficient to reduce sampling risk to an acceptably low level (AU-C 530.07). Our sampling approach documented the objectives of the test, population (including sampling unit and time frame), method used to select the sample, and sampling design and resulting sample size.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence (such as NLRB policies and procedures, system security plans, plan of actions and milestones, system reporting/dashboards, and system configurations) 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 2025 Inspector General FISMA metrics requirements, our testing concluded that NLRB has implemented an "effective" information security program for FY 2026. In comparison with the FY 2025 FISMA submission, the maturity levels for FY 2026 are as follows:

Fiscal Year 2025 & 2026 NLRB CyberScope FISMA Metrics Results		
Function	**Assessed Maturity Levels Fiscal Year 2025**	**Assessed Maturity Levels Fiscal Year 2026**
Function 1: Govern – Cybersecurity Governance / Cybersecurity Supply Chain Risk Management (C-SCRM)	Managed and Measurable	Managed and Measurable
Function 2: Identify – Risk and Asset Management (RAM)	Managed and Measurable	Managed and Measurable
Function 3: Protect – Configuration Management (CM) / Identity and Access Management (IDAM) / Data Protection and Privacy / Security Training	Optimized	Optimized
Function 4: Detect – Information Security Continuous Monitoring (ISCM)	Optimized	Optimized
Function 5: Respond – Incident Response	Managed and Measurable	Managed and Measurable
Function 6: Recover – Contingency Planning	Managed and Measurable	Managed and Measurable
Overall	**Effective**	**Effective**

V. FINDINGS AND RECOMMENDATIONS

Based on the FY 2026 FISMA audit results, our testing did not identify new deficiencies with respect to the effectiveness of the NLRB's security program and practices; however, we noted that three of the four recommendations from prior years remained open in FY 2026. See Appendix B, *FISMA Open Recommendations*.

VI. APPENDIX A – Management's Response

National Labor Relations Board (NLRB)
Federal Information Security Modernization Act Audit
For Fiscal Year 2026

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

Memorandum

To: **Ruth Blevins**
Inspector General

From: Prem Aburvasamy
Chief Information Officer

Date: August 18, 2026

Subject: OIG FISMA Audit Report – OIG-AMR-108

Management Response:

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report, 2026 Federal Information Security Modernization Act (FISMA) Audit for the National Labor Relation Board (NLRB), Report OIG-AMR-108. These audits provide an independent review of our operations and support our ongoing efforts to improve program security.

OCIO concurs with the three prior year's outstanding recommendations in the report which are listed below:

1. FY 2024-OIG-AMR-106-24-04. Recommendation #1 (Cybersecurity Supply Chain
2. Risk Management - Counterfeit Components).
3. FY 2025-OIG-AMR-107-25-01. Recommendation #1 (Risk and Asset Management - Data Management).
4. FY2025-OIG-AMR-107-25-01. Recommendation #3 (Incident Response - Event Logging)

OCIO is in the process of implementing corrective actions based on recommendations, contingent upon FY27 budget for necessary tools and resources.

OCIO received an "Effective" rating this year due to adequate funding, resources, and Agency Leadership support.

Thank you for the chance to respond. Please contact me with any questions or requests for more information.

VII. APPENDIX B – FISMA Open Recommendations

Fiscal Year - Audit No.	Recommendation Issued	Status in FY 2026
FY 2024 - OIG-AMR-106-24-04	Recommendation #1 (Cybersecurity Supply Chain Risk Management - Counterfeit Components)	Unresolved
FY 2025 - OIG-AMR-107-25-01	Recommendation #1 (Risk and Asset Management - Data Management)	Unresolved
FY 2025 - OIG-AMR-107-25-01	Recommendation #2 (Identity and Access Management - Privileged Account Reauthorization)	Resolved
FY 2025 - OIG-AMR-107-25-01	Recommendation #3 (Incident Response - Event Logging)	Unresolved