UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Memorandum

August 26, 2025

To: Prem Aburvasamy
Chief Information Officer

From: Ruth C. Blevins Ruth C Blevins
Inspector General

Subject: FY 2025 FISMA
(OIG-AMR-107-25-01)

This memorandum transmits the audit report "National Labor Relations Board (NLRB) Federal Information Security Modernization Act Audit for Fiscal Year 2025" 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 21, 2025, 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 recommendations. 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
Acting General Counsel
Audit Follow-up Official/Chief of Staff

National Labor Relations Board (NLRB)
Federal Information Security Modernization Act Audit
for Fiscal Year 2025

August 21, 2025

Submitted By:

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

Table of Contents

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, LLC (Castro & Co) was contracted by the NLRB's Inspector General to perform the NLRB's Fiscal Year (FY) 2025 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 Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, dated April 3, 2025. The FY 2025 Inspector General FISMA Reporting Metrics focused on 20 core metrics and five new 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 Office of Management and Budget (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". In addition, we made recommendations related to Risk and Asset Management, Identity and Access Management, and Incident Response. The recommendations were provided to the Office of the Chief Information Officer (OCIO) to strengthen and improve NLRB's information security program.

We caution that projecting the results of our audit to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance 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 to be and should not be used 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:

<table>
<tr><th colspan="2">NIST Cybersecurity Framework Alignment with the Fiscal Year 2025 IG FISMA Domains</th></tr>
<tr><th>NIST Cybersecurity Framework Functions</th><th>Fiscal Year 2025 IG FISMA Domains</th></tr>
<tr><td>Govern</td><td>Cybersecurity Governance
Cybersecurity Supply Chain Risk Management</td></tr>
<tr><td>Identify</td><td>Risk and Asset Management</td></tr>
<tr><td>Protect</td><td>Configuration Management
Identity and Access Management
Data Protection and Privacy Management
Security Training</td></tr>
<tr><td>Detect</td><td>Information Security Continuous Monitoring</td></tr>
<tr><td>Respond</td><td>Incident Response</td></tr>
<tr><td>Recover</td><td>Contingency Planning</td></tr>
</table>

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 2025. 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 2025 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. This review period was from October 1, 2024 through May 31, 2025.

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 were 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 staff in the OCIO 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 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 of selecting sample, and sample 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 2025. In comparison with the FY 2024 FISMA submission, the maturity levels for FY 2025 are as follows:

Fiscal Year 2024 & 2025 NLRB CyberScope FISMA Metrics Results		
Function	**Calculated and Assessed Maturity Levels** **Fiscal Year 2024**	**Calculated and Assessed Maturity Levels** **Fiscal Year 2025**
Function 1: Govern – Cybersecurity Governance / Cybersecurity Supply Chain Risk Management (C-SCRM)	N/A	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 & Privacy / Security Training	Optimized	Optimized
Function 4: Detect – Information Security Continuous Monitoring (ISCM)	Optimized	Optimized
Function 5: Respond – Incident Response	Optimized	Managed and Measurable
Function 6: Recover – Contingency Planning	Optimized	Managed and Measurable
Overall	**Effective**	**Effective**

V. FINDINGS AND RECOMMENDATIONS

Castro & Co identified three deficiencies in the general IT control area of Risk and Asset Management (Data Management), Identity and Access Management (Privileged Account Reauthorization), and Incident Response (Event Logging). During our review, we noted the following:

Risk and Asset Management (Data Management)

Based on testing performed and evidence reviewed, we noted that, as of the end of our audit, the NLRB's Enterprise Data Management Plan was in development. Additionally, the draft Enterprise Data Management Plan did not include a defined process for developing and maintaining comprehensive and accurate inventory data and corresponding metadata.

Furthermore, we noted the NLRB does not currently maintain a complete and accurate inventory of its data assets and associated metadata across its data types, where applicable.

According to Title 44 of the United States Code, Section 3511, titled *Data Inventory and Federal Data Catalogue,* federal agencies are required to develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, under the control or direction of, or maintained by the agency. The inventory must include metadata for each data asset, to the maximum extent practicable, such as a description (including variable names and definitions), name or title, disclosure status, agency or sub-agency responsible, asset owner, last update date, use restrictions, location, and any other metadata necessary to make the inventory useful to the agency and the public. Further, agencies are required to follow defined processes for updating and submitting the inventory and associated metadata for inclusion in the Federal Data Catalogue, as well as complying with any additional standards or guidance issued by the Director of OMB.

NLRB has not finalized and implemented its Enterprise Data Management Plan, resulting in the absence of a formally defined process for developing and maintaining comprehensive and accurate data inventories and associated metadata. OCIO stated that the NLRB does not have a Data Management Officer and/or Office/Program; therefore, the Enterprise (Agency) lacks a holistic Data Management Program.

The ongoing development of the NLRB's Enterprise Data Management Plan, coupled with the absence of a defined process for creating and maintaining a comprehensive and accurate inventory of data assets and corresponding metadata, increases the risk that the agency is unable to effectively manage, govern, and protect its data resources. Without a complete and accurate inventory, the NLRB may face difficulties protecting data quality, meeting federal data management requirements, and providing reliable information for decision-making and reporting purposes. This gap may also limit the NLRB's ability to safeguard sensitive data and comply with statutory obligations related to data management.

We recommend that the NLRB:

1. Finalize and formally implement the Enterprise Data Management Plan. At a minimum but not limited to, the Enterprise Data Management Plan should clearly define the processes and responsibilities for developing, maintaining, and updating a comprehensive and accurate inventory of all agency data assets and their associated metadata.

Identity and Access Management (Privileged Account Reauthorization)

NLRB has not performed the required annual review of privileged accounts to validate the continued need for elevated access privileges as required by the NLRB's policy.

NIST Special Publication 800-53 Revision 5 *(Security and Privacy Controls for Information Systems and Organizations – September 2020)* (NIST 800-53 Rev 5), Control AC-2 (Account Management) requires agencies to manage accounts throughout their lifecycle, including reviewing and validating the continued need for account privileges. NIST 800-53 Rev 5, Control AC-6(7) (Least Privilege | Review of User Privileges) requires the organization to periodically review privileged user accounts to confirm that elevated privileges remain necessary for users' job functions.

The OCIO stated that the annual review is performed as part of the NLRB Annual Privilege training (Privileged User Rules of Behavior Re-certification Training); however, the annual review was postponed.

Failure to regularly review privileged accounts increases the risk of unauthorized access and excessive privileges, which could lead to misuse or compromise of sensitive systems and data.

We recommend that the NLRB:

2. Complete an annual review of all privileged accounts to assess whether the elevated privileges remain necessary and promptly remove or adjust any access that is no longer required.

Incident Response (Event Logging)

NLRB did not achieve the required EL2 and EL3 event logging maturity levels by the deadlines established in OMB Memorandum M-21-31 primarily due to competing IT and cybersecurity priorities, limited resources and funding dedicated to upgrading logging infrastructure and tools, and challenges in coordinating efforts across systems and environment.

OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021), requires federal agencies to improve their investigative and remediation capabilities to ensure that enterprise security operation centers have centralized access to-and visibility into-system logs.

While NLRB has reached the Event Logging Tier (EL) EL1 maturity level, NLRB has not achieved the EL2 or EL3 maturity level in accordance with OMB-M-21-31 by OMB's deadlines as follows:

- Within 18 months of the date of OMB M-21-31, or by February 27, 2023, achieve the EL2 maturity level.
- Within two years of the date of OMB M-21-31, or by August 27, 2023, achieve the EL3 maturity level.

Comprehensive logging on federal information systems is critical for the timely detection, investigation, and remediation of cyber threats. By not achieving the required event logging maturity levels, the NLRB is not meeting OMB M-21-31 requirements for collecting logs at all criticality levels. As a result, there is an increased risk that the NLRB may fail to capture all meaningful and relevant data related to suspicious events, which could impede the agency's ability to appropriately identify, assess, and respond to potential security incidents or cyberattacks.

We recommend that the NLRB:

3. Implement requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.

VI. APPENDIX A – Management's Response

National Labor Relations Board (NLRB)
Federal Information Security Modernization Act Audit
For Fiscal Year 2025

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 19, 2025

Subject: OIG FISMA Audit Report – OIG-AMR-107

Management Response:

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report, 2025 Federal Information Security Modernization Act (FISMA) Audit for the National Labor Relation Board (NLRB), Report OIG-AMR-107. The OIG audits are always valuable as they afford us an independent assessment of our operations and help inform us of our continuous efforts to enhance the security of our program.

OCIO concurs with all three recommendations in the report which are listed below:

1. Finalize and formally implement the Enterprise Data Management Plan. At a minimum but not limited to, the Enterprise Data Management Plan should clearly define the processes and responsibilities for developing, maintaining, and updating a comprehensive and accurate inventory of all agency data assets and their associated metadata.

2. Complete an annual review of all privileged accounts to assess whether the elevated privileges remain necessary and promptly remove or adjust any access that is no longer required.

3. Implement requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.

The OCIO is addressing recommendation #2 by completing the annual review of all Agency privileged user accounts and launching Privileged User Security training courses.

The OCIO will proceed with the implementation of corrective actions to address recommendations #1 and #3, contingent upon the availability of budget necessary to procure the required tools and resources in FY26.

OCIO has received an overall rating of “Effective” this year. The rating was the direct result of sufficient budget funding, resources, and the support of Agency Leadership.

I appreciate the opportunity to respond to the draft report. Should you have any questions or require additional information regarding our response, please do not hesitate to contact me.