UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Memorandum

November 6, 2017

To: Philip A. Miscimarra
Chairman

Jennifer Abruzzo
Acting General Counsel

From: David P. Berry
Inspector General

Subject: Audit of the National Labor Relations Board Fiscal Year 2017 Financial Statements (OIG-F-22-18-01)

This memorandum transmits the audit report on the National Labor Relations Board (NLRB) Fiscal Year (FY) 2017 Financial Statements with the Management's Response.

The Accountability of Tax Dollars Act of 2002 requires the NLRB to prepare and submit to Congress and the Director of the Office of Management and Budget (OMB) annual audited financial statements. We contracted with Castro & Company, an independent public accounting firm, to audit the financial statements. The contract required that the audit be done in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and Bulletin 17-03, *Audit Requirements for Federal Financial Statements,* issued by OMB.

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 *Government Auditing Standards*, was not intended to enable us to express, and we do not express, opinions on the NLRB's financial statements or internal control or conclusions on compliance with laws and regulations. Castro & Company is responsible for the attached auditor's report dated November 6, 2017, and the conclusions expressed in the report. However, our review disclosed no instances where Castro & Company did not comply, in all material respects, with generally accepted government auditing standards.

The audit report states Castro & Company's unmodified opinion with regard to the FY 2017 and 2016 financial statements.

With regard to the Management Response dated November 3, 2017, and the apparent disagreement regarding the internal control findings, as stated in the audit reports, a deficiency in internal control exists when the design or operation of a control does not allow management or

employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A deficiency can exist in both the design and operation of an internal control:

A deficiency in design exists when:

- A control necessary to meet the control objective is missing; or
- An existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met.

A deficiency in operation exists when:

- A properly designed control does not operate as designed; or
- The person performing the control does not possess the necessary authority or competence to perform the control effectively.

A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

In applying the standards as set forth in the American Institute of Certified Public Accountants' *Statements on Auditing Standards* and the *Government Auditing Standards*, Castro & Company determined that the lack of required updated policies and procedures over security management and assessments, a security assessment that contained known or knowable misstatements of material fact, and the lack of a Contingency Plan and testing for information systems for achieving continuity of operations for mission/business functions during FY 2017 rose to the level of Material Weaknesses in both design and operation.

As noted in the Internal Control Report, the lack of formal policies and procedures increases the risk that the security practices are unclear, misunderstood, and improperly implemented; and that controls will be inconsistently applied in order to keep the NLRB information technology (IT) systems safe. Processing and storing financial information in weak or unsafe IT systems puts the NLRB's financial information and resources at risk of fraud, waste, and abuse. In addition, discrepancies may exist but go undetected and uncorrected, thereby causing the financial information to be misstated. Effective policies and procedures and management monitoring to ensure they are properly implemented greatly increases the NLRB's ability to proactively identify and resolve issues that could result in material misstatements in financial accounting and reporting records.

In addition, as stated in the Internal Control Report, during unscheduled disruptions in operations, the NLRB may not be able to recover and continue operation of all necessary systems and functions in a timely manner. Without an effective contingency plan in place for the general support system, the NLRB's financial data is at risk of being lost due to an unscheduled disruption. If lost financial data cannot be adequately restored, it could materially affect the financial statements.

Additionally, we found that NLRB management misquoted what the Internal Control Report stated in their response. The Report does not state that "the Agency has a variety of

sound practices in place regarding information technology policies and procedures," as noted in Management's response. The Report states that although NLRB "had some sound security practices in place, it did not have approved policies supporting practices placed in operation."

With regard to the Management Response for the finding related to the contractor oversight and security awareness training, National Institute of Standards and Technology Special Publication 800-53: PS-7 Third-Party Personnel Security requires that an agency establish personnel security requirements for third-party providers. The fact that the NLRB's Office of the Chief Information Officer (OCIO) did not have a definitive list of contractors during our audit indicates a lack of contractor oversight, and therefore the OCIO could not track contractors' compliance with security awareness training or the on/off-boarding processes.

With regard to the lack of a contingency plan and testing, the finding is not related to the Disaster Recovery Plan; as stated in the Management Response. It addresses the lack of a Contingency Plan as required by the Federal Information Security Modernization Act of 2014 (FISMA). Formulating a Contingency Plan is not only an improvement to the Agency's operations but is required to be in compliance with FISMA. The Internal Control Report states that while the Disaster Recovery Plan does address contingency plans related to the NLRB's information technology systems, its scope is limited to only catastrophic system failures and thus does not adequately address contingency procedures for all scenarios. In addition, it does not cover the NLRB's contingency responsibilities over the financial and payroll systems provided to them by the Department of the Interior. Any Contingency Plan put together by the Agency subsequent to the FY 2017 audit will be assessed during the FY 2018 audit.

As mentioned above, the issues identified above were a result of audit procedures conducted during our audit of the financial statements for FY 2017; therefore, corrective action initiated by the NLRB subsequent to the audit would be assessed as part of the FY 2018 audit.

We appreciate the courtesies and cooperation extended to Castro & Company and our staff during the audit.

Castro & Company
Auditors ✓ Advisors

1737 King Street
Suite 250
Alexandria, VA 22314
Phone: 703.229.4440
Fax: 703.859.7603
www.castroco.com

Independent Auditor's Report

Inspector General
National Labor Relations Board

We have audited the accompanying balance sheets of the National Labor Relations Board (NLRB) as of September 30, 2017 and 2016 and the related statements of net cost, changes in net position, and budgetary resources for the fiscal years then ended.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with U.S. generally accepted accounting principles; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with the auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and, Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the agency's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the agency's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant estimates made by management, as well as evaluating the overall presentation of the financial statements. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the NLRB as of September 30, 2017 and 2016, and the related statements of net cost, changes in net position, and budgetary resources for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Required Supplementary and Other Information

U.S. generally accepted accounting principles require that the information in the *Required Supplementary Information*, including *Management's Discussion and Analysis*, be presented to supplement the basic financial statements. Such information, although not part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board, who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. The supplementary information is the responsibility of management and was derived from, and relates directly to, the underlying accounting and other records used to prepare the basic financial statements. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audit of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

The information presented in the Messages from the Chairman, General Counsel, and Chief Financial Officer, list of Board Members, Other Accompanying Information, and Appendices is presented for purposes of additional analysis and are not required as part of the basic financial statements. Such information has not been subjected to auditing procedures applied by us in the audit of the basic financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Other Reporting Required by Government Auditing Standards

In accordance with U.S. *Government Auditing Standards* and OMB Bulletin No. 17-03, we have also issued our reports dated November 6, 2017, on our consideration of NLRB's internal control over financial reporting and the results of our tests of its compliance with certain provisions of laws, regulations, and other matters that are required to be reported under *Government Auditing Standards*. The purpose of those reports is to describe the scope of our testing of internal control over financial reporting and compliance and the results of that testing and not to provide an opinion on the internal control over financial reporting or on compliance. Those reports are an integral part of an audit performed in accordance with U.S. *Government Auditing Standards* and OMB Bulletin 17-03 in considering the NLRB's internal control and compliance, and should be read in conjunction with this report in considering the results of our audit.

This report is intended solely for the information and use of management and the NLRB Office of Inspector General, OMB, U.S. Government Accountability Office, and Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Castro & Company, LLC

November 6, 2017
Alexandria, VA

Castro & Company
Auditors ✓ Advisors

1737 King Street
Suite 250
Alexandria, VA 22314
Phone: 703.229.4440
Fax: 703.859.7603
www.castroco.com

Independent Auditor's Report on Internal Control

Inspector General
National Labor Relations Board

We have audited the financial statements of the National Labor Relations Board (NLRB) as of and for the year ended September 30, 2017, and have issued our report thereon dated November 6, 2017. We conducted our audit in accordance with the auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*.

In planning and performing our work, we considered the NLRB's internal control over financial reporting by obtaining an understanding of the design effectiveness of the NLRB's internal control, determining whether controls had been placed in operation, assessing control risk, and performing tests of the NLRB's controls as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not to express an opinion on the effectiveness of the NLRB's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the NLRB's internal control over financial reporting. We limited our internal control testing to those controls necessary to achieve the objectives described in the Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982 (FMFIA), such as those controls relevant to ensuring efficient operations.

Our consideration of internal control over financial reporting was for the limited purposes described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described below to be material weaknesses.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. During our audit we did not identify any deficiencies in internal control that we consider to be significant deficiencies. However, significant deficiencies may exist that have not been identified.

The NLRB's response to the findings identified in our audit is described in the accompanying Audit Response Letter. The NLRB's response was not subject to auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

We noted less significant matters involving internal control and its operations which we have reported to NLRB management in a separate letter dated November 6, 2017.

This report is intended solely for the information and use of the management and the NLRB Office of Inspector General, OMB, the Government Accountability Office, and Congress, and is not intended to be and should not be used by anyone other than these specified parties.

November 6, 2017
Alexandria, VA

MATERIAL WEAKNESSES

I. Lack of Information Technology Updated Policies and Procedures over Security Management and Assessments and Unreliable Security Assessment for the LAN/WAN General Support System

The head of each Federal agency is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, as described in the Federal Information Security Modernization Act (FISMA) of 2014 (PL 113-283, 44 USC 3554)[1]. Additionally, agency heads are responsible for reporting on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise. FISMA requires Federal agencies to improve the security of Information Technology (IT) systems, applications, and databases. Each Federal agency must develop, document, and implement a program to provide security for the data and IT systems that support its operations and assets. The National Institute of Standards and Technology (NIST) develops IT security standards and guidelines for FISMA. Federal agencies must follow these rules, which require compliance reporting by each agency. The NLRB is required to comply with FISMA.

The NLRB security controls were not effectively monitored or adequately documented, and system assessments and authorizations were not performed in accordance with Federal standards. The NLRB Office of the Chief Information Officer (OCIO) security personnel forwarded to the Chief Information Officer (CIO) a security assessment of the NLRB's LAN/WAN system with knowledge that the security assessment incorrectly stated that control policies and procedures were in place and were operating effectively when, in fact, they were not. The CIO then issued an Authority to Operate (ATO) for the LAN/WAN. Because it is the CIO's responsibility to approve the NLRB's IT security controls, he should have known that the security assessment that he was relying upon for the LAN/WAN ATO contained incorrect statements, and that the incorrect statements were material to his decision to accept the risks associated with the operation of the NLRB's LAN/WAN system.

During our review of the NLRB's policies and procedures and its independent security assessment of the LAN/WAN General Support System, we found the following:

Outdated Policies

NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4 has 18 controls specifically addressing policies and procedures. Policies and procedures are principles and rules to guide and direct employees and contractors in the performance of fulfilling their duties. Although NLRB had some sound security practices in place, it did not have approved policies supporting practices placed in operation. NLRB began the process of writing new policies and procedures for the NIST SP 800-53, Revision 4 control families, but no policy and procedures had been finalized, approved, or issued by the NLRB.

[1] The Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

NIST SP 800-53 was originally issued in 2005 and was last updated in 2013. The NLRB's policies and procedures currently in place predated the NIST SP 800-53 with the primary policy, Administrative Policies and Procedures Manual IT-1: Computer Security Program Information Systems Security Policy (INFOSYSEC), dating back to 2003.

Unreliable Security Assessment

- As part of the NIST Risk Management Framework (RMF), the NLRB is required to assess the effectiveness of controls in the System Security Plan (SSP) by an independent assessor. As such, the NLRB issued a contract to perform its Fiscal Year (FY) 2017 annual security assessment of the LAN/WAN General Support System. The Security Assessment Assessor stated in its report that controls were in place and in operation while both the NLRB OCIO security personnel and the Contractor's Assessor had full knowledge that some controls had not been implemented. The SSP and Security Assessment Report stated that the NLRB was following the policies and procedures controls for each of the 18 NIST SP 800-53 control families. Our testing found these policies and procedures were being developed; none of the policies and procedures were finalized, approved, or issued. The NLRB OCIO security personnel scheduled the completion of the policies and procedures for the 4th quarter of FY 2017 and the 2nd quarter of FY 2018. Both the NLRB OCIO and Assessor were aware of the draft status of those policies and procedures. Nonetheless, the assessment was certified stating that the policies and procedures were in place rather than documenting the lack of finalized policies and procedures. As a result, the security assessment contained incorrect information. The NLRB CIO then certified the ATO without noting the deficiency.

- The Assessor was required to test for effectiveness of control activities. For the controls we examined, the Assessor did not indicate they tested for effectiveness. In the assessment, the Assessor described the general control process that may have been in place. The Assessor did not specify that they selected samples to test individual control activities, nor did they specify the results of samples tested, if any. In addition, the Assessor did not test all required control activities listed under a control. For example, in testing control AC-2: Account Management, the Assessor did not mention the four (4) control enhancements included in AC-2. There is no evidence that these control enhancements were tested.

- During our review of the Security Assessment contract, we noted that the NLRB also agreed to the performance of additional tasks in that contract, which included performing Disaster Recovery Plan updates and testing, risk assessments, policy guidance and/or development, and transition planning. These additional services impaired the Contractor's independence in performing the security assessment. The Contractor must be impartial from the NLRB. Impartiality implies that the Contractor is free from any perceived or actual conflicts of interest pertaining to the development of procedures, operations, or management of information systems under assessment. In addition, impartiality implies that the Contractor is free from any perceived or actual conflicts of interest pertaining to the testing of the operating effectiveness of the security controls. To achieve impartiality, the Contractor should not have created a mutual or conflicting interest with the NLRB where it was conducting the assessment and evaluating its own work.

Contractor Oversight

The NLRB OCIO did not have a definitive list of contractors; therefore, they could not track contractors' compliance with security awareness training or the on and off-boarding processes. NLRB utilized an online training system to provide employees and contractors user access to several online training resources and to track completion of the required security awareness training for NLRB contractors. However, NLRB relied largely on manual processes initiated by administrative offices for tracking security awareness training and offboarding requirements for contractors.

Security Awareness Training

NLRB's Information Technology Security Education, Awareness and Training (ITSEAT), Standard and Implementation Guidelines states that "NLRB may elect to provide annual refresher material to contractors, however, the responsibility remains with the contractor to ensure annual refresher materials are provided to his or her employees as a part of the contract agreement. To assign this responsibility to the contractor, the following contractual language may be inserted into new and/or existing statements of work…The contractor must, at a minimum, certify that any personnel who perform work under this contract effort must have received annual IT Security awareness briefings as defined in NIST Special Publication 800-16 'Information Technology Security Training Requirements: A Role- and Performance-Based Model.' Certification of this training must be provided to the Associate CIO, IT Security no later than 45 calendar days after the training has occurred."

This control alone is insufficient to meet NIST requirements. It is NLRB's responsibility to monitor and enforce security controls.

Security assessments are important components of an organization-wide strategy. They determine whether security controls are implemented correctly, operating as intended, and producing the desired outcomes. They provide the basis for confidence in the effectiveness of security controls. Security assessments are a critical component supporting a system's ATO.

The Government Accountability Office's *Standards for Internal Control in the Federal Government* states:

> People are what make internal control work. The responsibility for good internal controls rests with all managers. Management sets the objectives, puts the control mechanisms and activities in place, and monitors and evaluates the control. However, all personnel in the organization play important roles in making it happen. All personnel need to possess and maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal control. Management needs to identify appropriate knowledge and skills needed for various jobs and provide needed training, as well as candid and constructive counseling, and performance appraisals.
>
> Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or

operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives…Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results…They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of the activities as well as appropriate documentation.

Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. Internal control serves as the first line of defense in safeguarding assets. In short, internal control helps managers achieve desired results through effective stewardship of public resources.

Management establishes physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment that might be vulnerable to risk of loss or unauthorized use. Management periodically counts and compares such assets to control records.

The NIST SP 800-53 Revision 4 requires that for each of the 18 control families that organizations develop policies and procedures. NIST SP 800-53 Revision 4 states,

1. Policies and Procedures:
   The organization:

   a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
      1. policies that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      2. Procedures to facilitate the implementation of the policies and associated specific controls; and

   b. Reviews and updates the current:
      1. Access control policy [*Assignment: organization-defined frequency*]; and
      2. Access control procedures [*Assignment: organization-defined frequency*].

   Supplemental Guidance: Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

NIST SP 800-53 Revision 4, CA-2 Security Assessments, has Control Assessment CA-2(1), Independent Assessors, which states:

> The organization employs assessors or assessment teams with [*Assignment: organization- defined level of independence*] to conduct security control assessments.
>
> Supplemental Guidance: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest about the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work…

NIST Special Publication 800-53A *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* Revision 4, Section 2.3 Building an Effective Assurance Case states,

> Building an effective assurance case for security and privacy control effectiveness is a process that involves: (i) compiling evidence from a variety of activities conducted during the system development life cycle that the controls employed in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements of the system and the organization; and (ii) presenting this evidence in a manner that decision makers are able to use effectively in making risk-based decisions about the operation or use of the system.

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4 states,

> AT-2 Security Awareness Training
>
> Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
>
> a. As part of initial training for new users;
> b. When required by information system changes; and
> c. Assignment: organization-defined frequency] thereafter.
>
> PS-7 Third-Party Personnel Security
>
> Control: The organization:
>
> a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and
e. Monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

The NLRB did not have adequate policies and procedures to ensure information system security due to the lack of management oversight over the security management program. The NLRB relied on outdated policies, to include policies dating back to 2003 that do not incorporate the most current NIST requirements. While the NLRB had begun to create some policies and procedures that conform to NIST SSP 800-53 Revision 4, they were still either in draft format or have not been started at all.

In addition, the NLRB CIO was not adequately managing his subordinate security personnel. The OCIO security personnel knowingly accepted and then used a security assessment that contained material misstatements of fact, and provided it to the CIO to use in authorizing the systems to operate.

It is apparent that NLRB was not aware or disregarded the need for a central control of contractor security requirements. The NLRB's current procedure tracked all users' security requirements through initial training, role-based training, and offboarding, but it did not specifically keep track of contractors. Often control of contractors' security requirements warranted communication and coordination with other administrative offices within an agency.

Without a strong tone at the top and proper management oversight to support the NLRB's IT system, there is a risk that control activities may not be appropriately designed or implemented. The establishment of written, formal policies and procedures is critical in assuring that a system of internal controls is followed.

The lack of formal policies and procedures increases the risk that the security practices are unclear, misunderstood, improperly implemented, and controls are inconsistently applied in order to keep the NLRB IT systems safe. Processing and storing financial information in weak or unsafe IT systems puts the financial information and resources at risk of fraud, waste, and abuse occurring. In addition, discrepancies may exist but go undetected and uncorrected, thereby causing the financial information to be misstated. Effective policies and procedures and management monitoring to ensure they are properly implemented greatly increases the NLRB's ability to proactively identify and resolve issues that could result in material misstatements in financial accounting and reporting records.

Without a proper independent assessment to determine the effectiveness of its security controls, the NLRB will not be able to determine the security posture of its operations and protect its operations.

Without a complete centralized list of contractors, NLRB cannot effectively monitor its contractors to ensure compliance with security awareness training or the on and off-boarding processes. There is an increased risk that some contractors may not be aware of NLRB security practices. The lack of monitoring of contractors leaving the Agency can also increase the risk that the contractors may not be removed timely from access lists and that NLRB property, including badges, are not returned timely, which could result in unauthorized access to the NLRB's general support system that houses its financial information.

Recommendations:

We recommend that NLRB management:

1. Establish, approve, and disseminate IT policies and procedures to all employees as required by NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* Revision 4. Final policies and procedures should have a clear audit trail showing signatures of individuals responsible for final approval and be dated accordingly.

2. Obtain an independent assessor to perform tests of effectiveness on all NLRB's SSP in accordance with NIST Special Publication 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Revision 4.

3. Review the knowledge, skills, and abilities of the OCIO security personnel and make a determination of whether individuals in those positions are skilled to perform IT security functions.

4. Develop a personnel policy that defines the NLRB's responsibility for maintaining a complete list of contractors that is periodically reviewed to ensure completeness and accuracy.

II. Lack of a Contingency Plan and Testing for Information Systems for Achieving Continuity of Operations for Mission/Business Functions

Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. We examined the NLRB's Disaster Recovery Plan version 9.6, dated November 22, 2016. While the Disaster Recovery Plan does address contingency plans related to the NLRB's information technology systems, its scope is limited to only catastrophic system failures and thus does not adequately address contingency procedures for all scenarios. In addition, it does not cover the NLRB's contingency responsibilities over the financial and payroll systems provided to them by the Department of the Interior. Although these systems are provided by a third-party, the NLRB is responsible for restoring connectivity and normal operations in the event of disruptions at the NLRB. The Disaster Recovery Plan makes explicit references to an IT Contingency Plan and a NLRB LAN/WAN Contingency Plan. Despite multiple requests for these documents, the NLRB was not able to provide them and we determined that neither an overall Contingency Plan nor an Information System Contingency Plan exists or is in place. NIST SP 800-53, Revision 4 requires that an organization develop and test a Contingency Plan annually, without a plan in place, no testing has been performed.

NIST SP 800-53 Rev. 4, CP-2 Contingency Plan states,

> Control: The organization:
>
> a. Develops a contingency plan for the information system that:
> 1. Identifies essential missions and business functions and associated contingency requirements;
> 2. Provides recovery objectives, restoration priorities, and metrics;
> 3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
> 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
> 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
> 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
>
> b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
>
> c. Coordinates contingency planning activities with incident handling activities;
>
> d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and

g. Protects the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

Control Enhancements:

(1) Contingency Plan | Coordinate with Related Plans

The organization coordinates contingency plan development with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

NIST SP 800-53 Rev. 4, CP-4 Contingency Plan Testing states,

> Control: The organization:
>
> a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
>
> b. Reviews the contingency plan test results; and
>
> c. Initiates corrective actions, if needed.
>
> Supplemental Guidance: Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. Related controls: CP-2, CP-3, IR-3.

The NLRB did not develop, approve, and disseminate Contingency Planning policies and procedures that provided guidance in the development and testing of a Contingency Plan.

The NLRB relied extensively on IT system controls to initiate, authorize, record, process, summarize, and report financial transactions in the preparation of its financial statements.

During unscheduled disruptions in operations, the NLRB may not be able to recover and continue operation of all necessary systems and functions in a timely manner. Without an effective contingency plan in place for the general support system, the NLRB's financial data is at risk of being lost due to an unscheduled disruption. If lost financial data cannot be adequately restored, it could materially affect the financial statements.

Recommendations:

5. Develop an overall contingency plan to include all NLRB systems, including the financial, payroll, Backpay and LAN/WAN systems.

6. Ensure that the contingency plan is tested, at a minimum once a year and that results of the test are reviewed so that corrective action can be initiated, if needed.

Castro & Company
Auditors ✓ Advisors

1737 King Street
Suite 250
Alexandria, VA 22314
Phone: 703.229.4440
Fax: 703.859.7603
www.castroco.com

Independent Auditor's Report on Compliance with Laws and Regulations

Inspector General
National Labor Relations Board

We have audited the financial statements of the National Labor Relations Board (NLRB) as of and for the year ended September 30, 2017, and have issued our report thereon dated November 6, 2017. We conducted our audit in accordance with the auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements.*

The management of NLRB is responsible for complying with laws and regulations applicable to NLRB. We performed tests of its compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts, and certain other laws and regulations specified in the Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements,* including the requirements referred to in the Federal Managers' Financial Integrity Act of 1982 (FMFIA). We limited our tests of compliance to these provisions, and we did not test compliance with all laws and regulations applicable to NLRB.

The results of our tests of compliance with applicable laws and regulations, and government-wide policies, described in the preceding paragraph identified instances of noncompliance that are required to be reported under *Government Auditing Standards* or OMB guidance, and are described in the following paragraphs.

The head of each Federal agency is responsible for providing information security protection commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, as described in the Federal Information Security Modernization Act (FISMA) of 2014 (PL 113-283, 44 USC 3554)[1]. Additionally, agency heads are responsible for reporting on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise. FISMA requires Federal agencies to improve the security of Information Technology (IT) systems, applications, and databases. Each Federal agency must develop, document, and implement a program to provide security for the data and IT systems that support its operations and assets. The National Institute of Standards and Technology (NIST) develops IT security standards and guidelines for FISMA.

[1] The Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

The NLRB security controls were not effectively monitored or adequately documented, and system assessments and authorizations were not performed in accordance with Federal standards. The NLRB did not have adequate policies and procedures to ensure information system security due to the lack of management oversight over the security management program. The NLRB relied on outdated policies, to include policies dating back to 2003 that did not incorporate the most current NIST requirements. While the NLRB had begun to create some policies and procedures that conform to NIST Special Publication (SP) 800-53 Revision 4, they were still either in draft format or have not been started at all.

NIST SP 800-53, Revision 4 also requires that an organization develop and test a Contingency Plan annually. However, the NLRB did not have an overall Contingency Plan nor an Information System Contingency Plan and without a plan in place, no testing has been performed. The NLRB did not develop, approve, and disseminate Contingency Planning policies and procedures that provided guidance in the development and testing of a Contingency Plan.

Providing an opinion on compliance with certain provisions of laws and regulations and government-wide policies was not an objective of our audit, and accordingly, we do not express such an opinion.

This report is intended solely for the information and use of management and the NLRB Office of Inspector General, OMB, Government Accountability Office, and Congress, and is not intended to be and should not be used by anyone other than these specified parties.

November 6, 2017
Alexandria, VA

UNITED STATES NATIONAL LABOR RELATIONS BOARD
OFFICE OF THE CHIEF FINANCIAL OFFICER

November 3, 2017

TO: David P. Berry, Inspector General

FROM: Mehul Parekh, Chief Financial Officer

SUBJECT: Response to the Audit of the National Labor Relations Board Fiscal Year 2017 Financial Statements

This letter is in response to the audit reports addressing the National Labor Relations Board (NLRB or Agency) Fiscal Year (FY) 2017 Financial Statements. The Agency has reviewed these reports including their findings and recommendations, and appreciates the opportunity to provide this response.

The auditor's opinion and determination confirmed that our financial statements represent fairly, in all material respects, the financial position of the NLRB as of September 30, 2017. We are pleased to see that the audit reflects the results that the Agency has achieved in meeting the goals set for FY 2017. The Office of the Chief Financial Officer continues to make progress in documenting its processes and procedures.

We have also reviewed your findings related primarily to computer system security procedures. As further discussed below, the Agency is committed to resolving in a diligent and effective manner the audit report's findings in this area, including issues relating to information technology policies and procedures, a FY 2017 security assessment, contractor oversight, security awareness training, contingency planning and testing for mission functions. In the Agency's view, these issues do not rise to the level of a material weakness although the Agency recognizes its responsibility to address all relevant concerns, and we provide the following additional information and observations.

The audit reports acknowledge that the Agency has a variety of sound practices in place regarding information technology policies and procedures, and the audit reports find that the Agency is updating these policies and procedures. In particular, the Agency had adopted an open Plan of Action and Milestones (POAM) for the purpose of updating NIST SP 800-53, Revision 4 control families. However, implementation of this Plan remains incomplete because of budgetary constraints, resource limitations, and competing priorities, especially those associated with the ongoing operation and maintenance of the Agency's information systems. We expect that significant steps towards completing the implementation of this POAM will occur in the current fiscal year, including effective documentation regarding relevant approvals and implementation.

With regard to the FY 2017 security assessment described in the audit report, the Office of the Chief Information Officer (OCIO) had adopted an open POAM to update control PM-1,

APPM IT-1 Computer Security Program Information Systems Security Policy (Infosysec), and security personnel in the OCIO were aware of this Plan, and there remain further efforts to address these issues based on staff and organizational restructuring and synchronizing a policy update with DHS's Continuous Diagnostics and Mitigation program. The Agency agrees with the recommendation to obtain an independent assessor to perform tests of effectiveness according to NIST SP 800-53A, and the Agency will ensure there is no conflict of interest associated with the procurement of such services.

With regard to contractor oversight and security awareness training, there is no guidance from NIST that training for contractors be tracked independently of any other type of user; and all system users are subject to our security awareness training program because the program is tied to the possession of a network account. For every new employee/contractor, the Associate CIO for Information Assurance and the Information Assurance analyst (not administrative offices) are responsible for initiating and documenting Cybersecurity Awareness training and annual refresher training. In subsequent audits, the Agency will ensure that the auditors receive relevant documentation regarding these types of training for all system users. The Agency continually assesses the performance of our personnel in all areas, and agrees with the recommendation that the Agency engage in an assessment within the OCIO, particularly as it relates to those individuals responsible for IT security functions.

As to contingency planning and testing, the Agency believes it is important to recognize that prior financial statement audits have found that the Agency's disaster recovery planning and exercise were sufficient. However, the Agency agrees it would be an improvement to formulate an overall contingency plan addressing all NLRB systems (including the Agency's financial, payroll, backpay and LAN/WAN systems), including regular testing and review of results. Thus, the Agency recently completed the development of such an overall contingency plan.

The Agency appreciates the significant work associated with these audits and the Agency remains committed to the continued refinement and improvement of processes, procedures, and policies to address the auditor's recommendations.

Mehul Parekh, Chief Financial Officer