

UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General



Memorandum

November 13, 2018

To: John F. Ring
Chairman

Peter B. Robb
General Counsel

From: David P. Berry 
Inspector General

Subject: Audit of the National Labor Relations Board Fiscal Year 2018 Financial Statements
(OIG-F-23-19-01)

This memorandum transmits the audit report on the National Labor Relations Board (NLRB) Fiscal Year 2018 Financial Statements with the Management 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 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 generally accepted government auditing standards issued by the Comptroller General of the United States and Bulletin 19-01, *Audit Requirements for Federal Financial Statements*, issued by the Office of Management and Budget.

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, 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 13, 2018, 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.

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

Independent Auditor's Report on the Financial Statements

Inspector General
National Labor Relations Board

We have audited the accompanying balance sheets of the National Labor Relations Board (NLRB) as of September 30, 2018 and 2017 and the related statements of net cost, changes in net position, and budgetary resources for the fiscal years then ended, and the related notes to the financial statements.

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. 19-01, *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 on the Financial Statements

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, 2018 and 2017, 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. 19-01, we have also issued our reports dated November 13, 2018, 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 19-01 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.



November 13, 2018
Alexandria, VA

Independent Auditor's Report on Internal Control over Financial Reporting Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*

Inspector General
National Labor Relations Board

We have audited the financial statements of the National Labor Relations Board (NLRB), which comprise the balance sheets as of September 30, 2018 and 2017, and the related statements of net cost, changes in net position, and budgetary resources for the years then ended, and the related notes to the financial statements, and have issued our report thereon dated November 13, 2018. We conducted our audit in accordance with 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. 19-01, *Audit Requirements for Federal Financial Statements*.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements as of and for the year ended September 30, 2018, we considered NLRB's internal control over financial reporting by obtaining an understanding of the design effectiveness of NLRB's internal control, determining whether controls had been placed in operation, assessing control risk, and performing tests of 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 NLRB's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of NLRB's internal control over financial reporting. We limited our internal control testing to those controls necessary to achieve the objectives described in the OMB Bulletin No. 19-01. 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.

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. 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.

Our consideration of internal control over financial reporting was for the limited purposes described in the first paragraph of this section and would not necessarily identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be significant deficiencies. We did identify two deficiencies in internal control, described below, that we consider to be material weaknesses.

NLRB's Response to Findings

NLRB's response to the findings identified in our audit is described in the accompanying Audit Response Letter. 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 13, 2018.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and the result of that testing, and not to provide an opinion on the effectiveness of NLRB's internal control. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering NLRB's internal control. Accordingly, this communication is not suitable for any other purpose.

This report is intended solely for the information and use of the management and 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.

A handwritten signature in black ink that reads "Castro & Company, LLC". The signature is written in a cursive, slightly slanted style.

November 13, 2018

Alexandria, VA

MATERIAL WEAKNESSES

I. Lack of Quality Control Procedures Caused Financial Reporting and Accounting Discrepancies

The Accountability of Tax Dollars Act of 2002 requires that NLRB submit audited financial statements to Congress and the Director of OMB on an annual basis. OMB Circular No. A-136, *Financial Reporting Requirements*, defines the form and content of financial statements to be prepared by NLRB that must also comply with Federal Accounting Standards. The statements must be prepared from an integrated financial management system containing sufficient structure, effective internal control, and reliable data. The financial reports must also be supported by comprehensive policies, with strong internal controls, that prescribe the procedures for processing and summarizing accounting entries, and preparing the financial statements.

As previously reported in Fiscal Year (FY) 2016, during our review of NLRB's financial statement preparation process during FY 2018, we identified issues that impacted NLRB's ability to effectively accumulate, assemble, and analyze information presented in its financial statements in accordance with applicable guidance. Examples of the errors noted include the following:

Financial Reporting

NLRB does not have sufficient resources to implement financial statement reporting requirements and sufficient controls in place to ensure that the financial statements are thoroughly prepared, reviewed, and presented in accordance with applicable requirements of OMB and Federal Accounting Standards, including the following:

- During our review of the financial statements and related crosswalks as of 6/30/2018, we identified an error on the reported balances for Imputed Financing Sources and Net Cost of Operations due to an incorrect journal voucher (JV) reversal of \$16.3M entered in January 2018. The JV reversed the Fourth Quarter 2017 Imputed Costs, which brought the Imputed Financing total to -\$1.5M on the Statement of Changes in Net Position (SCNP). After we brought the error to management's attention, a JV to correct the imputed cost to the correct balance of \$14.9M was recorded in August 2018.
- During our review of the financial statements and related crosswalks as of 9/30/2018, we identified that NLRB did not incorporate changes to the crosswalks for the SCNP and the Statement of Budgetary Resources (SBR) as required by the June 2018 Treasury Financial Manual (TFM) and the July 30, 2018 update of OMB Circular A-136, which are utilized to prepare the respective financial statements. Instead, NLRB management used the old crosswalks and modified the statements into the new presentation format. After we brought this to management's attention, the SCNP and SBR crosswalks were resubmitted in the updated format.

Journal Vouchers

We noted that NLRB did not follow quality control procedures over the preparation, review, approval or recording of JVs throughout the fiscal year. During our interim audit procedures, we noted the following:

- Various JVs above \$100,000 were posted to the general ledger (GL) prior to the secondary reviewer's approval as required by NLRB's internal policy. Similar exceptions were noted as of 9/30/2018;
- JVs were not adequately supported;
- Various JVs did not include an adequate detailed explanation for the purpose of the JV; and
- Various JVs related to Backpay were processed without an appropriate explanation for the reconciling differences. NLRB management processed these JVs period after period specifically to match the Governmentwide Treasury Account Symbol Adjusted Trial Balance System (GTAS) without researching the root cause of the differences; therefore, differences were not corrected in a timely manner.

Property, Plant, and Equipment (PP&E)

During our interim and year-end procedures, we noted that controls were not operating effectively to ensure PP&E accounts were properly reviewed and correctly reported on the financial statements, and as a result we noted the following:

- The PP&E reconciliation as of 6/30/18 and 9/30/18 lacked evidence of proper review and approval by NLRB Management.
- Incorrect amounts were reported for Construction-in-Progress (CIP) as of 6/30 and 9/30/18; specifically,
 - A difference of approximately \$36,000 was noted due to NLRB incorrectly recording the CIP amount for a Regional Office project based on a percentage of the original funded amount instead of the revised total funded amount. During the fiscal year, additional funding was approved for the project that increased the total cost, and as a result, an additional \$36,000 should have been recorded in CIP as of 6/30/18. This error was corrected as of 9/30/18 after we brought this to management's attention.
 - A difference of approximately \$56,000 was noted due to NLRB recording an approximate 65 percentage of completion for a Regional Office project instead of the correct 95 percent project completion of the total cost as of 9/30/18.

- A difference of approximately \$121,000 in Internal Use Software (IUS) as of 6/30/18 was noted as a result of NLRB incorrectly recording a JV reversal and retirement of approximately \$112,000 in IUS in order to correct an April 2017 booking of IUS additions in the Oracle Module. This error was brought to the attention of NLRB management as a result of the FY 2017 year-end audit procedures; however, the error had not been corrected as of 6/30/18 and was only corrected as of 9/30/18, after we brought this to management's attention.
- Documentation to support the retirement of one asset for an approximate cost of \$108,000 and the transfer of another asset with an approximate cost of \$24,000 at a loss of approximately \$7,000 was not provided for review as requested; therefore, we were unable to determine whether these transactions were valid. Additionally, NLRB management was unable to provide evidence of approval for the disposal and/or transfer of those assets. We noted that those assets were not included on the Capitalized Equipment Inventory memo dated April 16, 2018 from the Property Management Section confirming which assets should be removed from inventory due to surplus/transfer.

As part of the FY 2016 financial statement audit, we recommended that NLRB ensure all assets were properly recorded and depreciated to properly reflect asset, contra-asset, and expense balances. Additionally, we recommended that NLRB develop and implement standardized policies and procedures to ensure accountability, monitoring, and oversight of the PP&E disposals; however, the issues noted above as part of the FY 2018 financial statement audit confirm a lack of remediation of the prior year's finding.

Backpay

During our testing procedures of the Backpay balance as of 6/30/18 and 9/30/18, we performed a review of the Other Liabilities General Ledger account used to record fiduciary funds collected by NLRB and held in escrow accounts with the Treasury. Backpay funds administered by NLRB are used to provide a remedy to discriminatees when a violation of the National Labor Relations Act results in a monetary loss to discriminatees due to an unfair labor practice. The Backpay funds that are held by NLRB are received from a charged party/respondent. The Finance Branch disburses the Backpay funds when directed to do so by a Regional Office.

During our audit, we noted that NLRB did not always follow its policies and procedures to evidence proper review and approval of Backpay disbursement requests. Additionally, supporting documentation was not provided for all the disbursement transactions selected during our interim procedures; therefore, we were unable to determine whether the disbursements tested were valid as of 6/30/18.

Additionally, we noted reconciling differences of approximately \$86,000 as of 6/30/18 and \$102,000 as of 9/30/18 between balances reported in the Backpay Management System (BMS) and balances reported in Oracle Federal Financial (OFF) system and Treasury. NLRB management was not reconciling balances in the BMS to the balances in the OFF system on a monthly basis as required by NLRB's internal policy.

The issues noted above stem from the Finance Branch not having sufficient or adequate resources, nor having sufficient personnel with appropriate skill sets and expertise to perform financial management accounting and reporting throughout the fiscal year. Essential Finance personnel such as the Chief Financial Officer (CFO) position has been vacant since April 2018. The Supervisory Accountant position was vacant for six (6) months of the fiscal year. The vacant positions in the Office of the Chief Financial Officer (OCFO) for most of the fiscal year drastically hindered the OCFO's ability to effectively manage the financial operations of the Agency and ensure the reliability of financial reporting. During the course of our audit, it was not apparent that NLRB had a process in place to cross-train personnel to perform day-to-day financial accounting, analysis, review, and reporting tasks. Additionally, the Finance Branch did not have sufficient quality control procedures in place to detect certain financial reporting and accounting errors until they were brought to their attention by the auditors.

The Government Accountability's Office (GAO) *Standards for Internal Control in the Federal Government*, states

Personnel need to possess and maintain a level of competence that allows them to accomplish their assigned responsibilities, as well as understand the importance of effective internal control. Holding individuals accountable to established policies by evaluating personnel's competence is integral to attracting, developing, and retaining individuals.

Management performs ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions.

Management clearly documents internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination.

Management designs appropriate types of control activities for the entity's internal control system. Control activities help management fulfill responsibilities and address identified risk responses in the internal control system...

Management may design a variety of controls activities for operational processes, which may include verifications, reconciliations, authorizations and approvals, physical control activities, and supervisory control activities.

NLRB's *FY 2018 Backpay Cycle Memo*, states

An accountant reconciles the Backpay System case balances to the OFF system balances on a monthly basis.

NLRB's *Financial Manual, Journal Vouchers*, states

Approves the JV. The Oracle workflow, initiated by the Accountant, routes the JV to the Accounting Officer's queue for review and approval prior to posting. The Accounting Officer is notified that the JV is ready for approval when the Branch Chief provides the JV package. If the JV's total debits are larger than or equal to \$100k, the Accounting Officer forwards the JV to the CFO for approval; if not, the Accounting Officer approves the JV.

See also applicable criteria in:

- OMB Circular No. A-136, *Financial Reporting Requirements*
- Financial Accounting Standards Board (FASAB) Statement of Federal Financial Accounting Standards (SFFAS) No. 6, *Accounting for Property, Plant and Equipment*.

Without adequate staffing levels, the proper skill sets, and cross-training, the Finance Branch could continue to encounter challenges in its accounting and financial reporting processes. By not adequately performing management functions specific to monitoring, analysis, review, and oversight, discrepancies may exist but go undetected and uncorrected, thereby causing the financial information to be misstated. Effective management oversight greatly increases NLRB's ability to proactively identify and resolve issues that could result in misstatements in financial accounting and reporting records.

Recommendations:

We recommend that NLRB management:

1. Perform detailed management quality control reviews over the processing of JVs, year-to-year account balance variances, and accrual estimates to ensure discrepancies are minimized and errors are timely corrected.
2. Refine and strengthen policies, procedures, and processes over JVs and PP&E to ensure transactions are adequately supported and recorded accurately.
3. Ensure that reconciliations of the BMS balances to OFF and Treasury balances are completed, documented, and reviewed by management at a minimum on a quarterly basis.
4. Ensure reconciliations contain evidence of all appropriate reviews and approvals.

II. Lack of Sufficient General Information Technology Controls and Monitoring

GAO issued the Federal Information Systems Controls Audit Manual (FISCAM), which formed the basis for our Information Technology (IT) evaluation procedures. We used FISCAM as a guide to our audit as it informs financial statement auditors about IT controls and assists us in

planning our audit work. FISCAM controls are consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

The Federal Information Security Modernization Act (FISMA) of 2014 (PL 113-283, 44 USC 3554) requires Federal agencies to improve the security of 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. NIST develops IT security standards and guidelines for FISMA.

Our testing identified weaknesses in four general IT control subject areas: access control, segregation of duties, security management, and configuration management. During our review, we noted the following issues:

Access Control and Segregation of Duties

Access control is a fundamental component of information security for Federal information systems. It ensures that access control policies and programs are in place in order to protect financial data. Access control helps limit or detect inappropriate access and minimizes the risk of unauthorized access to information systems, which in turn protects systems from unauthorized modification, loss, and disclosure of financial data.

Audit logging and an effective incident response program is a fundamental component of information security for Federal systems. Audit logging ensures that auditable events are regularly collected, reviewed, and analyzed for indications of inappropriate or unusual activity. Reviews of audit logs should be done on a timely basis to ensure potential events or incidents are caught and resolved. Maintaining audit logs for a specified amount of time ensures that potential incidents can be further researched and followed-up on for resolution. Incidents should also be tracked and results of the analysis maintained in order to help security professionals routinely assess computer security, perform investigations during and after an attack, and recognize an ongoing attack to prevent future damage that could affect the confidentiality and integrity of financial data.

Segregation of duties is a fundamental component of internal controls. It ensures that work responsibilities are segregated so that one individual does not control all critical stages of a process, either IT or financial related.

During our audit procedures, we noted the following:

- There were no assigned account managers (those that approve accounts) for information systems accounts;
- There were no established conditions for groups and their role membership as well as a delineation showing separation of duties;
- Users' access forms were not maintained to show approvals and roles assigned;

- Although there was enough space to store the logs, audit logs were set to “overwrite” once they reached capacity, which creates/prevents investigations and audit follow-up in the event that an issue is identified;
- Audit logs were not being reviewed by authorized personnel on a prescribed basis; and
- A list of incidents being tracked was not provided; therefore, we were unable to ascertain whether NLRB tracks, documents, and reports potential incidents properly.

The Office of Chief Information Officer (OCIO) did not follow its own NLRB IT control policies AC-1, AU-1, IR-1, nor NIST SP 800-53 Revision 4, to assign account managers for information system accounts, establish conditions for group membership, maintain appropriate approval records and roles assigned for requests to establish accounts, and adequately implement appropriate audit log storage and audit log reviews.

Additionally, the OCIO did not provide documentation as requested for us to complete our audit procedures, which evidences their lack of tracking, documenting, and reporting potential incidents properly.

Security Management

Continuous monitoring of service organizations and complementary user entity controls (CUECs) not covered in the System and Organizational Controls (SOC1) report is important since these controls have not been tested in the SOC1 report. The user entity must and should evaluate those controls to ensure they are designed and operating effectively to ensure that financial data is not compromised and is accurate.

During our audit procedures, we noted the following:

- Continuous monitoring and/or controls analysis was not conducted for those controls not covered by the SOC1 report for OFF and Federal Personnel and Payroll System (FPPS) issued by the Department of the Interior.

NLRB did not have adequate controls in place to perform periodic assessments for controls not covered by the SOC1 report for OFF and FPPS. Additionally, NLRB has not documented policies and procedures to review the SOC1 reports and test CUEC from the SOC1 reports annually.

Configuration Management

Effectively monitoring and correcting known vulnerabilities is an important attribute of information security. Information systems should be scanned and updated in a timely manner to guard against vulnerabilities, missing patches, viruses, and other emerging threats that could potentially exploit the organization and financial data.

During our audit procedures, we noted the following:

- Vulnerabilities found on Agency vulnerability scan reports were not effectively monitored and timely remediated or corrected. Reports received from the OCIO showed there were several medium findings that had not been remediated from one month to the next.

NLRB did not have adequate controls in place to monitor the status of vulnerabilities identified. The following criteria relates to the conditions identified above:

- National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST 800-18, *Guide for Developing Security Plans for Federal Information Systems*, section 3.16
- GAO's *Standards for Internal Control in the Federal Government*, Principle 16 – Perform Monitoring Activities
- NLRB *Information Security Risk Assessment Policy, No. RA-1* issued January 18, 2018
- NLRB's *Information Security Assessment and Authorization Policy, No. CA-1* issued January 17, 2018
- NLRB's *Information Security Audit and Accountability Policy, No. AU-1* issued March 6, 2018
- NLRB's *Information Security Incident Management Policy, No. IR-1* issued October 12, 2017
- NLRB's *Information Security Access Control Policy, No. AC-1* issued October 3, 2017

Without account managers it could be harder to identify the personnel who are authorized to approve information system user accounts. Furthermore, without proper documentation for conditions as it relates to groups and their role membership, and maintaining user access forms, there is an increased risk that users will be granted roles in excess of what they should have to perform their normal job duties. Lastly, this could create an environment where a user could potentially exploit NLRB's financial systems and data.

If audit logs are overwritten once the logs fill up, this could prevent subsequent investigations, as the audit log will have been deleted. Additionally, if audit logs are not reviewed, the Agency might not be able to detect and report suspicious activities that could lead to the lack of financial data integrity and adversely affect the financial statements.

By not ensuring the tracking and maintenance of respective incidents, the Agency could be ill prepared to manage and respond to future incidents that could potentially affect financial data.

By not performing periodic assessments for controls not covered by the SOC1, there is an increased risk of exploitation because specific controls are not being assessed and/or monitored by NLRB or a third-party provider, which could in turn lead to a lack of financial data integrity for NLRB.

By having vulnerabilities exposed to the agency and not remediated in a timely manner, there is the risk that adversaries can take advantage of those weaknesses and gain access to NLRB's data, which ultimately could lead to a lack of integrity and/or confidentiality of financial data for the agency.

Recommendations:

5. Ensure that there are account managers assigned (and documented) to all personnel so that users' access rights are approved by an authorized person at the Agency.
6. Document all users' access rights and their respective segregation of duties to ensure that as users are approved, they are not being assigned privileges in excess of what their job duties require.
7. Document and maintain user access request forms, showing approvals and roles assigned.
8. Ensure that the audit logs are moved to another storage medium so that the audit logs are always available if needed for investigative purposes.
9. Review, analyze and report potential suspicious activities in the audit logs (by authorized personnel) on a monthly basis.
10. Track and maintain a record of all information system security incidents.
11. Develop and implement policies and procedures to review the SOC1 reports annually.
12. Identify controls that are not covered by the SOC1 report for OFF and FPPS and ensure they are assessed at least annually.
13. Establish controls to monitor or track the status of vulnerabilities identified.
14. Establish or modify the policy for how timely deficiencies (high, medium, and low) need to be remediated. Best practices across other agencies remediate high vulnerabilities within one business day and medium vulnerabilities within 3-5 business days; therefore, NLRB should follow best practices.

**Independent Auditor's Report on Compliance and Other Matters Based on an Audit of
Financial Statements Performed in Accordance with *Government Auditing Standards***

Inspector General
National Labor Relations Board

We have audited the financial statements of the National Labor Relations Board (NLRB), which comprise the balance sheets as of September 30, 2018 and 2017, and the related statements of net cost, changes in net position, and budgetary resources for the years then ended, and the related notes to the financial statements, and have issued our report thereon dated November 13, 2018. 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. 19-01, *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 OMB Bulletin No. 19-01, including the requirements referred to in the Federal Managers' Financial Integrity Act of 1982. We limited our tests of compliance to these provisions, and we did not test compliance with all laws and regulations applicable to NLRB.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the NLRB's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, and contracts, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests of compliance disclosed no instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 19-01.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of compliance and the results of that testing, and not to provide an opinion on the NLRB's compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the NLRB's compliance. Accordingly, this communication is not suitable for any other purpose.

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.

Castro & Company, LLC

November 13, 2018
Alexandria, VA

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



November 13, 2018

TO: David P. Berry
Inspector General

FROM: Beth Tursell
Acting Chief Financial Officer

SUBJECT: Response to the NLRB 2018 Draft Internal Control Report

The purpose of this memorandum is to respond to the Office of Inspector General's (OIG's) Draft Fiscal Year 2018 Internal Control Report. As further discussed below, the Agency is committed to resolving, in a diligent and effective manner, the audit report's findings. 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. Accordingly, we provide the following responses.

Recommendations

1: Perform detailed management quality control reviews over the processing of JVs, year-to-year account balance variances, and accrual estimates to ensure discrepancies are minimized and errors are timely corrected.

Response:

- The OCFO will continue to document processes and improve accuracy and timeliness of reporting obligation and accounts payable balances.

2. Refine and strengthen policies, procedures, and processes over JVs and PP&E to ensure transactions are adequately supported and recorded accurately.

Response:

- The OCFO will continue its practice of ensuring JVs are adequately supported and recorded accurately. The OCFO will implement controls to ensure evidence of review and approval by NLRB Management of PP&Es.

3. Ensure that reconciliations of the BMS balances to OFF and Treasury balances are completed, documented, and reviewed by management at a minimum on a quarterly basis.

Response:

- The OCFO will review policies and procedures to incorporate the quarterly review of BMS balances to OFF and Treasury balances.

4. Ensure reconciliations contain evidence of all appropriate reviews and approvals.

Response:

- The OCFO will continue its practice of ensuring evidence of review and approval by NLRB Management of reconciliations.

5. Ensure that there are account managers assigned (and documented) to all personnel so that users' access rights are approved by an authorized person at the Agency.

Response:

- The OCIO will review IT system access procedures for Agency managed systems. Information System owners will be documented, and account manager identified by the respective system owners.

6. Document all users' access rights and their respective segregation of duties to ensure that as users are approved, they are not being assigned privileges in excess of what their job duties require.

Response:

- OCIO will work with individual IT System owners to document account approval processes to include the separation of duties.

7. Document and maintain user access request forms, showing approvals and roles assigned.

Response:

- The OCIO will access the ability to centralize the request, documentation and recording of IT system access requests. Additional funding may be required to purchase "approver/reviewer" licenses as account managers and information system owners are added to approval processes per system.

8. Ensure that the audit logs are moved to another storage medium so that the audit logs are always available if needed for investigative purposes.

Response:

- The OCIO will review storage retention requirements for audit logs and provide sufficient storage. The OCIO will refine AU procedures to safeguard the storage of audit log data for investigative purposes.

9. Review, analyze and report potential suspicious activities in the audit logs (by authorized personnel) on a monthly basis.

Response:

- The OCIO will review audit logs for suspicious behavior on a monthly basis for analysis and reporting of suspicious activities.

10. Track and maintain a record of all information system security incidents.

Response:

- The OCIO will review Incident Handling, and Risk Strategy procedures to ensure system security incidents are documented.

11. Develop and implement policies and procedures to review the SOC1 reports annually.

Response:

- The OCIO will review policies and procedure to incorporate the annual review of vendor provided SOC1 reports.

12. Identify controls that are not covered by the SOC1 report for OFF and FPPS and ensure they are assessed at least annually.

Response:

- The OCIO will identify non-covered controls for OFF and FPPS based on the assessment of vendor provided SOC1 reports.

13. Establish controls to monitor or track the status of vulnerabilities identified.

Response:

- Subject to the availability of funding, The OCIO plans to purchase in-house tools for the monitoring and remediation of vulnerabilities. The OCIO will review potential vendor products to supplement DHS CDM activities.

14. Establish or modify the policy for how timely deficiencies (high, medium, and low) need to be remediated. Best practices across other agencies remediate high vulnerabilities within one business day and medium vulnerabilities within 3-5 business days; therefore, NLRB should follow best practices.

Response:

- The OCIO will revise Risk Management, and Incident Response procedures to include quantitative metrics for the remediation of vulnerabilities. Response times will be established based on the nature, risk, impact, and cost of remediation. The OCIO will revise procedures to remediate legitimate vulnerabilities dependent on criticality based on vendor and Federal guidance and in accordance with an organizational assessment of risk.

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.

A handwritten signature in black ink, appearing to read "Beth Tursell", written over a horizontal line.

Beth Tursell, Acting Chief Financial Officer