NATIONAL LABOR RELATIONS BOARD

Fiscal Year 2018 Financial Statement Audit

Management Letter Report

Castro & Company
Auditors ✓ Advisors

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

November 13, 2018

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 and have issued our report thereon dated November 13, 2018.

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 noted certain matters involving internal control and other operational matters that are summarized in this letter. These comments and recommendations, all of which have been discussed with the appropriate members of management and the NLRB Office of Inspector General, are intended to improve internal control or result in other operating efficiencies.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses or deficiencies in internal control, policies or procedures that may exist.

We would like to express our appreciation to you and all other NLRB personnel who assisted us in completing our work.

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

Sincerely,

Castro & Company, LLC

Castro & Company, LLC
Alexandria, VA

1. Improvements in the Management of Government Charge Cards Are Needed (Repeat Condition from FY 2014, FY 2015 and FY 2017)

As part of our testing of cash disbursements, we selected a sample of 45 disbursements made during the period of 10/1/17 through 3/31/18. The purpose of our testing was to assess management controls and compliance with applicable laws, regulations, and procedures relative to cash disbursement transactions. The following condition was noted:

- NLRB did not always oversee the completion of the required GSA SmartPay/refresher training. Specifically, we noted that for one (1) purchase cardholder and three (3) travel cardholders tested, the GSA certifications on file were completed more than three years ago.

NLRB's purchase and travel cardholders are required to complete GSA SmartPay/refresher training at a minimum every three (3) years; however, some cardholders did not consistently complete the GSA SmartPay/refresher training within the required three (3) years.

In prior fiscal years, we recommended that NLRB management review, implement, and monitor control activities related to the training of cardholders. Additionally, we recommended that NLRB management establish and implement procedures for the periodic review of all active cardholders to determine whether each cardholder has a need for the purchase/travel card, and whether all applicable documentation, including completion of initial and refresher trainings, is maintained. We reviewed management's corrective action plan regarding these recommendations and determined that adequate monitoring of control activities related to the training of cardholders and management's review of the cardholder files had not been completed as of our testing in May 2018.

The *Government Charge Card Abuse Prevention Act of 2012,* enacted in October 2012, states,

> § 1909(a) The head of each executive agency that issues and uses purchase cards and convenience checks shall establish and maintain safeguards and internal controls to ensure the following:
>
> (1) There is a record in each executive agency of each holder of a purchase card issued by the agency for official use, annotated with the limitations on single transactions and total transactions that are applicable to the use of each such card or check by that purchase card holder….
> (8) Periodic reviews are performed to determine whether each purchase card holder has a need for the purchase card.
> (9) Appropriate training is provided to each purchase card holder and each official with responsibility for overseeing the use of purchase cards issued by the executive agency.
> (10) The executive agency has specific policies regarding the number of purchase cards issued by various component organizations and categories of component organizations, the credit limits authorized for various categories of card holders, and categories of employees eligible to be issued purchase cards, and that those policies are designed to minimize the financial risk to the Federal Government of the issuance of the purchase cards and to ensure the integrity of purchase card holders.

Office of Management and Budget (OMB) Circular A-123, Appendix B, Revised, *Improving the Management of Government Charge Card Programs*, states,

> [E]ach agency must develop and maintain written policies and procedures for the appropriate use of charge cards consistent with the requirement of this guidance. The plan should be updated annually, or more frequently, if necessary to maintain current. Agencies shall submit a copy of their plan to OMB, Office of Federal Financial Management, on an annual basis, not later than January 31 of each calendar year.

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

> 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.
>
> 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 should remediate identified internal control deficiencies on a timely basis.

The establishment of written, formal policies and procedures are critical in assuring that a system of internal controls is followed. The lack of monitoring compliance with established procedures can increase the risk of fraud, waste, and abuse occurring in government charge cards.

Recommendations:

Our testing confirmed a lack of remediation of previous years' findings; therefore, new recommendations are not deemed necessary at this time.

Management's Response:

NLRB concurs with the findings related to the management of charge cards. The Office of the Chief Financial Officer (OCFO) addressed training concerns in both the Purchase Card Program and the Travel Card Program. With the transition from GSA SmartPay 2 Program to GSA SmartPay 3 Program cardholders are in process of taking a series of training courses to include GSA's updated charge card program training materials. Purchase Cardholders will complete the GSA training by the end of the third quarter of FY 19 due to the overwhelming amount of system and programmatic trainings they are required to take. Travel Cardholders have less of a

systematic burden and are scheduled to complete the GSA training by the end of FY 19. In the Spring of FY 19 the OCFO will release the Charge Card Program Policy and Charge Card Management Plan. Both documents will address internal controls and periodic program reviews of both Purchase and Travel Programs. This is also addressed in the Corrective Action Plan tracker.

Auditor's Response:

The auditors concur with management's response.

2. Inadequate Controls over Undelivered Orders and Accounts Payable (Repeat Condition from FY 2014 (Material Weakness), FY 2015, FY 2016 (Significant Deficiency) and FY 2017 (Management Letter))

During our testing of Undelivered Orders (UDO) and Accounts Payable (A/P), we selected a sample of 22 UDO transactions as of 9/30/18. The purpose of our testing was to assess management controls and compliance with applicable laws, regulations, and procedures relative to the NLRB's open obligations and corresponding accruals in order to support the validity of UDO balances. The results of our year-end testing identified the following exceptions in five (5) of the 22 transactions tested:

- Differences noted as a result of incorrect accruals: Three (3) under-accruals totaling $233,887 that understated the A/P balance and overstated the UDO balance and two (2) over-accruals totaling $19,321 that overstated the A/P balance and understated the UDO balance as of 9/30/18.

Additionally, we selected a sample of 23 UDO transactions as of 6/30/18. The results of our interim testing identified the following exceptions in eight (8) of the 23 transactions tested. Exceptions noted included the following:

- Differences noted as a result of incorrect accruals: Three (3) under-accruals totaling $213,219 that understated the A/P balance and overstated the UDO balance and five (5) over-accruals totaling $267,615 that overstated the A/P balance and understated the UDO balance as of 6/30/18.

GAO's *Standards for Internal Control in the Federal Government* states,

> 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.
>
> Transactions are promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from its initiation and authorization through its final classification in summary records. In addition, management designs control activities so that all transactions are completely and accurately recorded.

> Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained.
>
> Management perform 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. Ongoing monitoring may include automated tools, which can increase objectivity and efficiency by electronically compiling evaluations of controls and transactions.
>
> Management should remediate identified internal control deficiencies on a timely basis.

Statement of Federal Financial Accounting Standards No. 1, *Accounting for Selected Assets and Liabilities*, states,

> Accounts payable are amounts owed by a Federal entity for goods and services received from, progress in contract performance made by, and rents due to other entities…When an entity accepts title to goods, whether the goods are delivered or in transit, the entity should recognize a liability for the unpaid amount of the goods. If invoices for those goods are not available when financial statements are prepared, the amounts owed should be estimated.

31 U.S.C § 1501 (a)(1) states, in part, that an amount shall be recorded as an obligation of the United States Government only when supported by documentary evidence of a binding agreement between the agency and another person, including an agency, that is in writing and executed before the end of the period of availability of the funds.

Not performing an accurate review of open obligations, expenditures, and accounts payable resulted in an under/overstatement in A/P and under/overstatement in the obligations. Additionally, the financial data used to generate management and financial reports required by applicable laws and regulations was not accurate. As a result, those charged with governance did not have reliable financial information to manage the operations of the Agency.

Recommendations:

Our testing confirmed a lack of remediation of previous years' findings; therefore, new recommendations are not deemed necessary at this time.

Management's Response:

NLRB concurs with the findings and recommendations related to UDOs and accounts payable. The OCFO continues to address the internal control issues identified. Standard Operating Procedures were provided for the Accrual Process which encompasses portions of the UDO process. The OCFO is in the process of preparing additional guidance which will include a

flowchart of the UDO process and internal controls. Additionally, the Invoice Processing Platform (IPP), which was mandated by Treasury this year, was partially implemented by the NLRB (as a pilot). Currently, there are seven vendors in the IPP for the NLRB. The Agency will document the recommendations and options to mitigate the issues identified.

Auditor's Response:

The auditors concur with management's response.

3. Improvement in General Information Technology Controls and Monitoring over Security Management, Configuration Management, and Contingency Planning Are Needed

Our testing identified other matters involving internal control and its operations in three general IT control subject areas: security management, configuration management and contingency planning. During our review, we noted the following issues:

Security Management

Security management is the foundation of an entity's overall information security program, which also reflects senior management's commitment to addressing information security risks. It provides a framework and the means for a continuing cycle for managing risk, developing security polices, assigning information security responsibilities, and monitoring the adequacy of the NLRB's computer-related controls.

Security management provides a framework and the means for a continuing cycle for managing risk, developing security polices, assigning information security responsibilities, and monitoring the adequacy of the NLRB's computer-related controls.

During our audit procedures, we noted the following:

- The signed Rules of Behavior form was not provided for all employees tested. Additionally, the Rules of Behavior established by the NLRB did not include the provisions and/or restrictions for posting on social media/networking sites or on public websites.

- The security awareness training material does not include topics on recognizing and reporting potential indicators of insider threats.

The Office of the Chief Information Officer (OCIO) did not follow its own NLRB IT control policies PL-1, AT-1, nor NIST 800-53 Revision 4, to ensure that all users (employees and contractors) provide a signed acknowledgment indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system and the security awareness training include recognizing and reporting potential indicators of insider threats.

Configuration Management

Configuration management is an important attribute to information security and systems as it helps to prevent unauthorized changes to information system. Procedures and processes should be thoroughly documented as well as baseline configurations of information systems in order to have an effective configuration management program.

During our audit procedures, we noted the following:

- A baseline configuration was not maintained, and periodic reviews were not conducted to ensure that the baseline had not changed;
- A Configuration Management Plan was not documented; and
- There was no detailed information system components' inventory such as versions, manufacturer, model, serial number, the physical location of the components, and assigned personnel responsible for maintaining those components.

The OCIO did not follow its own NLRB IT control policy CM-1, nor NIST 800-53 Revision 4, to adequately document and/or assess all Configuration Management controls.

Contingency Planning

Contingency planning is a fundamental component for overall information security for federal systems. This control helps to protect information resources and minimize risk of unplanned interruptions, such as natural disasters or power outages. It also provides for recovery of critical operations should any interruptions occur.

During our audit procedures, we noted the following:

- Information was not maintained to evidence that backups are tested periodically.
- Future maintenance was not scheduled on information systems and components.

The OCIO did not follow its own NLRB IT control policies CP-1, MA-1, nor NIST 800-53 Revision 4, to test the backups on a periodical basis and schedule and perform future maintenance.

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*
- *NLRB Information Security Risk Assessment Policy, No. PL-1* issued December 13, 2017
- *NLRB Cybersecurity Awareness and Training Policy, No. AT-1* issued August 4, 2017
- *NLRB Information Security Configuration Management Policy, No. CM-1* issued October 12, 2017

- *The NLRB Information Security Contingency Planning Policy, No. CP-1* issued October 31, 2017
- The *NLRB Information Security Maintenance Policy, No. MA-1* issued January 30, 2018

By not ensuring that all the users accessing the systems know their roles, responsibilities, and expected behavior (including the stipulation for social media and posting on network sites), the risk that employees and contractors will be unaware of their roles and responsibilities is increased. Without knowledge of their roles and responsibilities, it further increases the risk that the Agency will be exposed to unforeseen risks through the sharing, posting or dissemination of data, which can be used for subsequent exploitation and may lead to a lack of financial data integrity and confidentiality for the Agency.

Failure to ensure that all users take yearly training on recognizing and reporting potential indicators of insider threats increases the risk of compromise with regard to confidentiality, integrity or availability of the organization's financial data or network systems.

By not maintaining and documenting a consistent baseline, there is the risk that as changes are made to the environment, configuration changes will be made without a rollback option.

By not developing an Agency Configuration Management Plan, there is the risk that changes will be made to Agency systems without following approved procedures of ensuring that changes are reviewed, tested, and approved prior to migrating them to production. This may ultimately impact those respective financial systems where unauthorized or unapproved changes were made, resulting in potential data (financial) loss.

By not ensuring a detailed system component inventory is maintained, the risk of duplicate components is increased, thereby not reflecting an accurate picture of the current information system inventory.

If the Agency does not test the backups periodically, there is a risk that damaged financial data may not be restored properly.

By not having scheduled future maintenance and performing this maintenance accordingly, this may impact the longevity of the endpoints being managed by the Agency that could affect financial data.

Recommendations:

We recommend that NLRB management:

1. Revise the Rules of Behavior to include social media, networking sites, posting on commercial websites and sharing of data.

2. Ensure all employees and contractors sign the latest revised Rules of Behavior as evidence of their acceptance.

3. Update and include recognizing and reporting potential indicators of insider threats in the security awareness training.

4. Create and document a baseline configuration for at least the last two baselines. Additionally, ensure that those baselines are periodically reviewed for completeness and accuracy.

5. Develop a detailed Configuration Management Plan to include items such as the types of changes, approval process, testing procedures/process, and proper migration of the change to the production environment, etc.

6. Ensure that the latest list representing the information system component inventory includes elements such as hardware inventory specifications (manufacturer, device type, model, serial number, and physical location), software license information, software version numbers, component owners, etc.

7. Ensure that backups are tested and documented at least annually.

8. Schedule future maintenance and perform them according to the schedule.

Management's Response:

NLRB concurs with the findings and recommendations related to Security Management, Configuration Management, and Contingency Planning, and offers the following consolidated response to the enumerated recommendations:

Recommendations 1 & 2: The OCIO will revise the Rules of Behavior to include social media, networking sites, posting on commercial websites and sharing of data. The revised Rules of Behavior will be incorporated into the Agency's annual Cybersecurity Awareness training to ensure all employee/contractor awareness and continued compliance.

Recommendation 3: The OCIO has obtained a learning management system to expand IT Security training content. The OCIO will revise its IT Security Training curriculum – to update and include recognizing and reporting potential indicators of insider threats in the security awareness training.

Recommendation 4: The OCIO has a baseline configuration for Windows 10 workstations and Microsoft Azure cloud server. The OCIO will expand configuration documentation to include network configuration baselines and document the baseline configuration of current production state systems. The OCIO will utilize a Configuration Management Plan (CMP), and Vulnerability Monitoring related procedures to address configuration review periods.

Recommendation 5: The OCIO will develop a CMP to include items such as the types of changes, approval process, testing procedures/process, and proper migration of the change to the production environment, etc., and update the related Change Management procedures in support of CMP procedures.

Recommendation 6: A Configuration Management Database is currently used to track manufacturer, device type, model serial number and physical location inventory elements as applicable. The OCIO will review Configuration Management Database processes and procedures to incorporate the recording of software license information, version numbers, components, etc., as applicable per component.

Recommendation 7: The OCIO will review policies and revise procedures to ensure Agency managed system backups are tested annually.

Recommendation 8: Maintenance activities for internally managed systems are scheduled per patch management, and Information Technology (IT) System release project schedules. Maintenance contracts for third party services are performed on a break/fix or as-needed basis. The OCIO will review Change Management procedures to ensure maintenance activities for third party services are documented.

Auditor's Response:

The auditors concur with management's response.

Status of Prior Year Management Letter Comments

The Fiscal Year (FY) 2017 and 2014 Management Letter Reports issued by Castro & Company identified the following control deficiencies:

Fiscal Year	Finding Identified	Status in FY 2018
FY 2014	Improvements in the Internal Controls over the Management of Government Charge Cards are Needed	Partially Resolved
FY 2014	Improvements in the Internal Controls over the Management and Monitoring of Negative Leave are Needed	Resolved
FY 2017	Inadequate Controls over Undelivered Orders and Accounts Payable	Partially Resolved
FY 2017	Inadequate Management Review and Oversight Which Caused Deficiencies in Finalizing and Submitting the NLRB FY 2017 Performance and Accountability Report (PAR) to OMB Timely	Partially Resolved

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

January 4, 2019

TO: David P. Berry
Inspector General

FROM: Beth Tursell
Acting Chief Financial Officer

SUBJECT: Response to Draft 2018 Management Letter

The National Labor Relations Board (NLRB) has reviewed the Draft FY18 Management Letter and concurs with the report's findings and recommendations. The Agency responses to each of the areas of concern are provided below. The NLRB leadership looks forward to working with the Office of Inspector General in closing out these items at the earliest possible time.

#1 Improvements in the Management of Government Charge Cards Are Needed (Repeat Condition from FY 2014, FY 2015 and FY 2017)

Management Response: NLRB concurs with the findings related to the management of charge cards. The Office of the Chief Financial Officer (OCFO) addressed training concerns in both the Purchase Card Program and the Travel Card Program. With the transition from GSA SmartPay 2 Program to GSA SmartPay 3 Program cardholders are in process of taking a series of training courses to include GSA's updated charge card program training materials. Purchase Cardholders will complete the GSA training by the end of the third quarter of FY 19 due to the overwhelming amount of system and programmatic trainings they are required to take. Travel Cardholders have less of a systematic burden and are scheduled to complete the GSA training by the end of FY 19. In the Spring of FY 19 the OCFO will release the Charge Card Program Policy and Charge Card Management Plan. Both documents will address internal controls and periodic program reviews of both Purchase and Travel Programs. This is also addressed in the Corrective Action Plan tracker.

#2 Inadequate Controls over Undelivered Orders and Accounts Payable (Repeat Condition from FY 2014 (Material Weakness), FY 2015, FY 2016 (Significant Deficiency) and FY 2017 (Management Letter))

Management Response: NLRB concurs with the findings and recommendations related to UDOs and accounts payable. The OCFO continues to address the internal control issues identified. Standard Operating Procedures were provided for the Accrual Process which encompasses portions of the UDO process. The OCFO is in the process of preparing additional guidance which will include a flowchart of the UDO process and internal controls. Additionally, IPP, which was mandated by Treasury this year, was partially implemented by the NLRB (as a pilot). Currently, there are seven vendors in IPP for the NLRB. The Agency will document the recommendations and options to mitigate the issues identified.

3. Improvement in General Information Technology Controls and Monitoring over Security Management, Configuration Management, and Contingency Planning Are Needed

Management Response: NLRB concurs with the findings and recommendations related to Security Management, Configuration Management, and Contingency Planning, and offers the following consolidated response to the enumerated recommendations:

Recommendations 1 & 2: The OCIO will revise the Rules of Behavior to include social media, networking sites, posting on commercial websites and sharing of data. The revised Rules of Behavior will be incorporated into the Agency's annual Cybersecurity Awareness training to ensure all employee/contractor awareness and continued compliance.

Recommendation 3: The OCIO has obtained a learning management system to expand IT Security training content. The OCIO will revise its IT Security Training curriculum – to update and include recognizing and reporting potential indicators of insider threats in the security awareness training.

Recommendation 4: The OCIO has a baseline configuration for Windows 10 workstations and Microsoft Azure cloud server. The OCIO will expand configuration documentation to include network configuration baselines and document the baseline configuration of current production state systems. The OCIO will utilize a Configuration Management Plan (CMP), and Vulnerability Monitoring related procedures to address configuration review periods.

Recommendation 5: The OCIO will develop a CMP to include items such as the types of changes, approval process, testing procedures/process, and proper migration of the change to the production environment, etc., and update the related Change Management procedures in support of CMP procedures.

Recommendation 6: A Configuration Management Database is currently used to track manufacturer, device type, model serial number and physical location inventory elements as applicable. The OCIO will review Configuration Management Database processes and procedures to incorporate the recording of software license information, version numbers, components, etc., as applicable per component.

Recommendation 7: The OCIO will review policies and revise procedures to ensure Agency managed system backups are tested annually.

Recommendation 8: Maintenance activities for internally managed systems are scheduled per patch management, and Information Technology (IT) System release project schedules. Maintenance contracts for third party services are performed on a break/fix or as-needed basis. The OCIO will review Change Management procedures to ensure maintenance activities for third party services are documented.

Respectfully submitted,

ELIZABETH TURSELL

Digitally signed by ELIZABETH TURSELL
Date: 2019.01.04 15:13:42 -05'00'

Beth Tursell, Acting Chief Financial Officer