NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Charlie Janssen
State Auditor

Charlie.Janssen@nebraska.gov
PO Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
www.auditors.nebraska.gov

January 30, 2019

Kyle Schneweis, Director
Nebraska Department of Transportation
1500 Nebraska Hwy 2
Lincoln, Nebraska 68502

Dear Mr. Schneweis:

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the State of Nebraska (State), as of and for the year ended June 30, 2018, in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, we have issued our report thereon dated January 4, 2019. In planning and performing our audit, we considered the State's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements of the State, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

In connection with our audit described above, we noted certain internal control or compliance matters related to the activities of the Nebraska Department of Transportation (Department) or other operational matters that are presented below for your consideration. These comments and recommendations, which have been discussed with the appropriate members of the Department's management, are intended to improve internal control or result in other operating efficiencies.

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 a 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.

Our consideration of internal control included a review of prior year comments and recommendations. To the extent the situations that prompted the recommendations in the prior year still exist, they have been incorporated in the comments presented for the current year. All other prior year comments and recommendations (if applicable) have been satisfactorily resolved.

Our consideration of internal control was for the limited purpose described in the first paragraph and was not designed to identify all deficiencies in internal control 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 material weaknesses or significant deficiencies. However, material weaknesses or significant deficiencies may exist that were not identified.

In addition, we noted other matters involving internal control and its operation that we have reported to management of the Department, pursuant to AICPA Auditing Standards AU-C Section 265.A17, in a separate early communication letter dated September 27, 2018.

Draft copies of this letter were furnished to the Department to provide management with an opportunity to review and to respond to the comments and recommendations contained herein. All formal responses received have been incorporated into this letter. Responses have been objectively evaluated and recognized, as appropriate, in the letter. Responses that indicate corrective action has been taken were not verified at this time, but they will be verified in the next audit.

The following are our comments and recommendations for the year ended June 30, 2018.

1. Capital Asset Acquisitions

During testing of the Department's capital assets, we noted the following:

- One asset's date of acquisition was not updated appropriately, causing depreciation expense to be overstated by $41,296 in the accounting system.

- The Department did not assign costs to five assets, totaling $1,949,819, in a timely manner. Costs were not added to the accounting system until after October 2018. Two of the assets' assigned dates of acquisition were prior to fiscal year 2018, being November 2016 and April 2017, respectively. However, those assets were placed into service during fiscal year 2018; therefore, the dates of acquisition should have been updated. The incorrect dates caused depreciation expense to be overstated by $92,478 for fiscal year 2017 and understated by $469,163 for fiscal year 2018.

Good internal controls require adequate policies and procedures to ensure capital assets are properly recorded for financial reporting requirements.

Without these procedures, there is an increased risk of material misstatement of the financial statements.

> We recommend the Department ensure asset acquisition dates are properly recorded in the State's accounting system, and all costs are entered timely for assets placed into service.

Department Response: NDOT concurs and will improve processes to ensure capital asset acquisition dates are properly recorded and costs are entered timely.

2. Risk Assessment

The Department was in the process of developing an Information Technology (IT) Security Plan to include an IT risk assessment; however, the plan was not completed as of the fiscal year ended June 30, 2018.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, 8-206 (July 2017), states, in relevant part, the following:

> *Agencies must perform a periodic threat and risk assessment to determine the security risks to facilities that contain state information, and implement reasonable and appropriate physical security measures to prevent and detect unauthorized access, theft, damage or interference.*

NITC Technical Standards and Guidelines, 8-703(1) (July 2017), states, in relevant part, the following:

> *This policy is based on the NIST SP 800-53 security controls framework. Pursuant to that framework, the state must conduct an annual review of the information technology environment to ensure compliance with these standards. The security controls that are to be inspected are organized into control families within three classes (management, operational, and technical).*
>
> *The state information security officer will facilitate and oversee an annual security control assessment. This assessment will cover at least 1/3 of the control areas defined in the NIST SP 800-53 security controls, such that over a three-year timeframe all control areas will have been assessed. This review must be conducted for each major system used within the state, and must include all infrastructure and peripheral processes that are used to support state business processes.*

NITC Technical Standards and Guidelines, 8-904 (July 2017), provides the following:

> *Each agency shall perform a security control assessment that assesses the adequacy of security controls for compliance with this policy and any applicable security frameworks (e.g., NIST, PCI, CMS, and IRS). The assessment may be performed internally by the agency information security officer or with the assistance of the state information security officer. Each agency is required to have an assessment at least once every year, covering at least one-third of the applicable controls such that all control areas have been assessed over a three-year period. Agencies are also required to perform an assessment anytime significant changes to the technical environment occur.*

A good internal control plan requires procedures to ensure that an IT risk assessment is completed and updated periodically.

Without adequate risk assessment procedures, there is an increased risk that an application's threats will not be identified. This increases the risk of preventable security vulnerability and threat exploitation, causing such issues as downtime, loss of productivity, unauthorized access, compromise of confidential information or data integrity, or interference with other State or Federal systems.

A similar finding was noted during the previous audit.

> We recommend the Department complete its IT Security Plan and implement procedures to ensure the periodic performance of an IT risk assessment that addresses application-specific risk information.

Department Response: BTSD continues to work toward completion of an application-specific risk assessment for NDOT. BTSD had previously delayed completion of its specific IT Security Plan until revisions to the NITC Security Policy were complete. Recent consolidation of BTSD's network resources having moved to OCIO and the subsequent role of network security coverage and responsibilities provided by OCIO remains unclear at this time. BTSD has, in the past, reached out to OCIO's State Security Officer for direction and in doing so continues to address and implement appropriate changes to applications to mitigate security vulnerability risk for NDOT. BTSD anticipates completion of an IT Security Plan by 2nd quarter of this calendar year.

* * * * *

Our audit procedures are designed primarily on a test basis and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. Our objective is, however, to use our knowledge of the Department and its interaction with other State agencies and administrative departments gained during our work to make comments and suggestions that we hope will be useful to the Department.

This communication is intended solely for the information and use of the Department, the Governor and State Legislature, others within the Department, Federal awarding agencies, pass-through entities, and management of the State of Nebraska and is not intended to be, and should not be, used by anyone other than the specified parties. However, this communication is a matter of public record, and its distribution is not limited.

Philip J. Olsen, CPA, CISA
Assistant Deputy Auditor