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 24, 2017

Kyle Schneweis, Director
Nebraska Department of Roads
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, 2016, 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 December 15, 2016. 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 Department of Roads (Department) or other operational matters that are presented below for your consideration. The 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.

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 the Department's internal control that we consider to be material weaknesses or significant deficiencies. However, material weaknesses or significant deficiencies may exist that were not identified.

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, 2016.

1. Required Supplementary Information Errors

During testing, it was noted that the estimated costs of maintaining roads at, or above, the established condition was originally reported at $347 million; however, the correct figure was $317 million, based on supporting documentation provided by the Department. The variance between the two figures was due to incorrectly calculating the interstate portion of the calculation, using total miles of State roads instead of strictly the interstate miles.

A good internal control plan requires procedures to ensure that information provided for the State of Nebraska Comprehensive Annual Financial Report (CAFR) is accurate and properly supported.

Without adequate procedures in place to ensure the accuracy of the financial reports and information used to prepare the CAFR, there is an increased risk of material misstatement.

> We recommend the Department implement policies and procedures to ensure that all information provided for the CAFR is accurate and properly supported.

Department Response: The Department concurs with the recommendation. This process is being documented and we expect to have this data available through the BICC performance measures initiative currently under way.

2. State Contract Database

During testing, we noted six contracts were not viewable on the State contract database website. For contracts to appear on the website, the Department is responsible for scanning copies into the State's enterprise content management system known as Onbase. The Department noted technical issues with its automated process to upload contracts. The Department subsequently provided the contracts upon request.

Neb. Rev. Stat § 84-602.04(1) (Cum. Supp. 2016) states, in relevant part, "The State Treasurer shall develop and maintain a single, searchable web site with information on state receipts, expenditures of state funds, and contracts which is accessible by the public . . . ." Subsection (4)(a)(i) of that same statute requires the Treasurer's web site to link to the web site of the Department of Administrative Services, which must contains a "data base that includes a copy of each active contract that is a basis for an expenditure of state funds, including any amendment to such contract and any document incorporated by reference in such contract." That subsection also requires the following:

The data base shall be accessible by the public and searchable by vendor, by state entity, and by dollar amount. All state entities shall provide to the Department of Administrative Services, in electronic form, copies of such contracts for inclusion in the data base beginning with contracts that are active on and after January 1, 2014 . . . .

When contracts are not scanned into the State's contract database in a timely manner, valuable information is not available to the Legislature or the general public, as intended by State statue.

We recommend the Department continue to work with the Office of the Chief Information Officer to ensure all contracts are viewable on the State contract database website.

Department Response: The Department concurs with the recommendation. The Construction Division has just completed the project to electronically upload the contracts into the LB429 data base.

3. Information Technology (IT) Risk Assessment

We noted the Department is in the process of developing an Information Technology Security Plan that includes an IT risk assessment; however, that assessment lacks application-specific risk information. The Department has multiple applications, which may have different levels of risk.

A similar finding was noted during the previous audit.

NITC Standards and Guidelines, Information Security Policy 8-101 (December 10, 2013), Section 4.5.1, Physical Security Perimeter, states, in relevant part, the following:

Agencies will perform a periodic threat and risk assessment to determine the security risks to facilities that contain State information . . . .

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.9.3, Risk Assessment, states, in relevant part, the following:

Security requirements and controls must reflect the value of the information involved, and the potential damage that might result from a failure or absence of security measures . . . . The framework for analyzing the security requirements and identifying controls to meet them is associated with a risk assessment, which must be performed by the data owner(s) and Agency management. A process must be established and implemented for each application to:

- *address the business risks and develop a data classification profile to help to understand the risks;*
- *identify security measures based on the criticality and data sensitivity and protection requirements;*
- *identify and implement specific controls based on security requirements and technical architecture;*
- *implement a method to test the effectiveness of the security controls; and*
- *identify processes and standards to support changes, ongoing management and to measure compliance.*

A good internal control plan requires procedures to ensure that an IT risk assessment is completed and updated periodically. Those procedures should require the assessment to address application-specific risk information.

Without such 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.

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

Department Response: NDOR continues to work on its formal IT Security Plan and risk assessment process. NDOR's resident network team has been relocated to the OCIO, and with this, NDOR has a dependency upon the OCIO to provide guidance, services, and detail for an enterprise solution / plan that would engage multiple agencies. In the meantime, NDOR has reached out to the Department of Labor for input regarding their use of vendor Veracode security software for performing vulnerability assessments of applications. Since the fall of 2016, NDOR has had numerous discussions and demos from Veracode and are now working on a proof of concept (POC). Should the POC prove viable, NDOR may seek to purchase software and/or select services from Veracode. NDOR is actively compiling an inventory of its applications and dependent systems, to be used in the further evaluation of application security/vulnerability assessment.

4. Terminated User Accounts

The Department had 387 employee terminations for the fiscal year ended June 30, 2016. For 2 of 19 terminations selected for testing, we noted the users' access was not deleted from the network in a timely manner (within three business days). The delay in deleting the access for the two users was 178 business days and 5 business days, respectively.

A similar finding was noted during the previous audit.

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, states the following, in relevant part:

> *A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (read, write, delete, etc.). The "Principle of Least Privilege" should be used to ensure that only authorized individuals have access to applications and information and that these users only have access to the resources required for the normal performance of their job responsibilities . . . .*
>
> *Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.*

A good internal control plan includes a process to ensure terminated users' network access is removed timely.

When access to networks and applications is not terminated timely, it creates the opportunity for inappropriate access to State resources.

> We recommend the Department remove terminated user network access immediately.

Department Response: BTSD personnel continue to follow appropriate termination activities. The two exceptions noted are explained below:

- *The 178 business day delay for Amanda Giles' (temporary employee) was due to BTSD not being notified in a timely manner by HR.*

  BTSD received its notification from HR on 7/20/16 that her last day had been 10/30/15. BTSD deleted the ID on 7/20/16, upon the notification.

- *Chi Chows' last day was 3/14/2016 and the ID was deleted on 3/21/2016. BTSD received the notification on 3/18/16, which is within the three business days compliance from notification.*

5. Change Management

The Department had 60 changes to the Roads Billing System (RBS), Roads Payment System (RPS), and Project Finance System (PFS) during the fiscal year tested. Four of nine changes tested were not authorized by appropriate management. One of these changes was not authorized, and the other three changes were authorized by the same person who developed and tested the change.

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.9.11, Change Control Management, states the following, in relevant part:

> *To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all change before implementation and ensure that accurate documentation is maintained. These change control procedures will apply to agency business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.*

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.3.2.3, Separation of Duties, states the following, in relevant part:

> *To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical. Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, audit trails and management supervision must be implemented.*

Without proper and consistent change control standards and segregation of duties, changes to an application may be made without specific management approvals. This could lead to data loss, compromised financial data integrity, or unintended system downtime. There is an increased risk that a change could be developed and moved into production without separate review and approval.

> We recommend the Department implement procedures to ensure that all changes made to IT systems are properly approved, and such changes are not developed, tested, and authorized by the same individual.

Department Response: Upon notification that there had been several inappropriate approvals take place by one individual, BTSD took immediate action to remove this permission level, as well as reviewed all permissions levels. This review found just the one individual as having incorrect permissions. Further research concluded that this individual was granted permission to authorize change management requests by his supervisor, so as to enable customer support while the supervisor was out of the office dealing with immediate family health issues. BTSD management was unaware that this authorization level had been granted, and the supervisor in question has since retired. With regard to the one change that was not authorized, further research concluded that this was an instance where the change was implemented without appropriate authorization. BTSD changes are reviewed with regularity (Tuesdays of each week), wherein all change impacts and schedule are discussed prior to implementation. This review of implementations is available on the internal intranet 'Interchange' - Project List/Change Management.

* * * * *

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
Audit Manager