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 23, 2018

Rhonda Lahm, Director
Nebraska Department of Motor Vehicles
301 Centennial Mall South, 1st Floor
Lincoln, Nebraska 68509

Dear Ms. Lahm:

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, 2017, 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 14, 2017. 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 Motor Vehicles (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 November 27, 2017.

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. The Department declined to respond.

The following are our comments and recommendations for the year ended June 30, 2017.

1. Unknown Destination of "Due to" Funds

The Department was unable to identify the proper destination of a portion of its "due to" funds. An International Registration Plan (IRP) liability balance of $495,658 and an International Fuel Tax Agreement (IFTA) liability balance of $114,362 existed at June 30, 2017. The Department did not know the destination of these funds. State IRP funds are distributed in accordance with Neb. Rev. Stat. § 60-3,202 (2016 Cum. Supp.). State IFTA funds are credited to the Motor Carrier Services Division Distributive Fund per Neb. Rev. Stat. § 66-1414 (Reissue 2009), which is reported in the Highway Fund for CAFR reporting purposes. We proposed an adjustment to record the liability balances as revenue consistent with the referenced statutes.

Neb. Rev. Stat. § 60-3,202, states:

> *(1) As registration fees are received by the Division of Motor Carrier Services of the department pursuant to section 60-3,198, the division shall remit the fees to the State Treasurer, less a collection fee of three percent of thirty percent of the registration fees collected. The collection fee shall be credited to the Department of Revenue Property Assessment Division Cash Fund. The State Treasurer shall credit the remainder of the thirty percent of the fees collected to the Motor Vehicle Tax Fund and the remaining seventy percent of the fees collected to the Highway Trust Fund.*

Neb. Rev. Stat. § 66-1414, states:

> *(1) Any fuel tax collected pursuant to the agreement shall be remitted to the State Treasurer for credit to the Motor Carrier Services Division Distributive Fund to carry out the International Fuel Tax Agreement Act.*

Sound accounting practices and a good internal control plan require policies and procedures to be in place to ensure the Department is aware of those to whom funds are owed.

Without such policies and procedures, there is an increased risk of loss or misuse of State and/or other jurisdiction funds.

We recommend the Department implement procedures for reviewing "due to" funds to ensure these amounts are appropriately allocated.

2. Application Change Management

During testing of the Department's change management process for the Motor Carrier Services (MCS), Vehicle Titling and Registration (VTR), and Traffic Safety Information (TSI) applications, we noted the following:

- **MCS Application**: One developer was responsible for the change management process. This developer was able to perform all change management functions and could develop a change and move it to production without involving anyone else.

- **VTR Application**: The Department used the Implementer tool to track and implement changes to the application. We noted three Department user IDs had move and checkout access to the VTR development, test, and production environments.

  For 1 of 10 changes tested, there was not adequate documentation to support that two individuals were involved with and aware of the change or to support that the change was approved prior to migration to production.

- **TSI Application**: The Department used the Implementer tool to track and implement changes to the application. We noted two Department user IDs had move and checkout access to the TSI development, test, and production environments.

  The Department used the Change Control Facility/Migration Management Facility (CCF/MMF) tool for tracking changes made to the TSI application. During a review of access to the CCF/MMF tool, four users were identified who had access to check out code, develop a change, promote the change, and move the change into production. The APA also noted that two terminated users had access to the CCF/MMF tool. These users had an active Resource Access Control Facility (RACF) ID and access to CCF/MMF for 143 and 35 business days after their respective termination dates.

A similar finding was noted during the previous audit.

Nebraska Information Technology Commission (NITC) Standards & Guidelines, Information Security Policy 8-101(December 2013), Section 4.9.11, Change Control Management, states the following:

> *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 changes 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 & Guidelines, Information Security Policy 8-101(December 2013), Section 4.3.2.3, Separation of Duties, states the following:

> *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. At a minimum, the audit of security must remain independent and segregated from the security function.*

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.7.2, User Account Management, states, in relevant part, the following:

> *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.*

Without proper and consistent change control standards and a 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 also an increased risk that a change could be developed and moved into production without involvement by a separate individual. When access to applications is not terminated timely, it creates an opportunity for inappropriate access to State resources.

> We recommend the Department develop and implement a formalized change management process for MCS and TSI applications. The process should include documented change requests, testing procedures, and management approval to implement the change into production. We also recommend the Department implement a process to document who developed, tested, approved, and moved changes to production for all changes to the VTR application. We recommend the Department implement an adequate segregation of duties to prevent a single user from checking out code, developing, and promoting changes to the point where the Office of the Chief Information Officer moves the change to production. Lastly, we recommend the Department implement procedures to ensure a user's access to the CCF/MMF tool is removed upon his or her termination.

* * * * *

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