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
auditors.nebraska.gov

December 19, 2019

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, 2019, in accordance with auditing standards generally accepted in the United States of America and the 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 19, 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 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 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.

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. A significant deficiency is a deficiency, or 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 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. However, material weaknesses may exist that have not been 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, 2019.

1. Capitalization of Computer Software

The Department incorrectly expensed costs, totaling $14,660,000, for internally generated computer software that should have been capitalized in accordance with Governmental Accounting Standards Board (GASB), Statement 51, *Accounting and Financial Reporting for Intangible Assets*. The costs were incurred from April 2018 through June 2019. The Department did not have policies and procedures for the review of internally generated software to determine which costs were appropriate to be expensed versus capitalized in accordance with GASB and the Department of Administrative Services (DAS) policies.

GASB Statement 51 provides, in relevant part, the following:

> *7. Intangible assets are considered internally generated if they are created or produced by the government or an entity contracted by the government, or if they are acquired from a third party but require more than minimal incremental effort on the part of the government to begin to achieve their expected level of service capacity.*
>
> * * * *
>
> *9. Computer software is a common type of intangible asset that is often internally generated. Computer software should be considered internally generated if it is developed in-house by the government's personnel or by a third-party contractor on behalf of the government. Commercially available software that is purchased or licensed by the government and modified using more than minimal incremental effort before being put into operation also should be considered internally generated for purposes of this Statement.*

The DAS State Accounting Manual, General Policies, Section 28, "Capital Outlay," states, in relevant part, the following:

> *[C]omputer software that is internally developed or substantively modified, shall be capitalized as a separate asset if the acquisition value is One Hundred Thousand Dollars ($100,000) or more and has a life greater than one year.*

Good internal controls require procedures to ensure that internally generated software is properly expensed or capitalized in accordance with GASB and DAS policies.

Without such procedures, there is an increased risk of the financial statements being materially misstated.

> We recommend the Department implement procedures to ensure internally generated software is properly expensed or capitalized in accordance with GASB and the State Accounting Manual.

Department Response: Prior to expensing the $14,660,000 for the new Vehicle Title and Registration System (VicToRy); the agency Controller had conversations with the State Accounting Office. Appropriate journal entries will be made to correct the costs which were incorrectly expensed. A meeting has already occurred with State Accounting to identify procedures for similar expenses in the future.

2. VTR County Users

During testing, we obtained a listing of all county Vehicle Title and Registration system (VTR) users and selected six counties to verify the employment status of each county's VTR users. From the counties' responses, we tested users whose employment was identified as having been terminated. We noted that 11 of 18 county VTR user IDs had not had their access disabled. Furthermore, 6 of 18 user IDs had a sign-on date after the employees had been terminated. These six user IDs were either shared among county staff or used by another employee after a previous employee had been terminated.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, Information Security Policy 8-502 (July 2017), "Minimum user account configuration," states the following, in relevant part:

> *(1) User accounts must be provisioned with the minimum necessary access required to perform duties. Accounts must not be shared, and users must guard their credentials.*

NITC Technical Standards and Guidelines, Information Security Policy 8-303(3) (July 2017), "Identification and authorization," says, "Sharing user IDs is prohibited."

Good internal control requires procedures to ensure that each VTR user ID is disabled timely upon termination of the employee to whom it was assigned and is not shared with other employees.

Without such procedures, there is an increased risk of not only unauthorized access to VTR but also inability of the Department to account for system user activity.

> We recommend the Department implement procedures to ensure that the VTR terminated user IDs are disabled in a timely manner. In addition, we recommend the Department communicate with counties that user IDs should not be shared.

Department Response: The department put in place a process to periodically review user accounts to the VTR System. In addition the County Treasurers are advised at meetings and workshops of their responsibility to notify the department when an employee is no longer employed. Those procedures are also outlined in the operating manuals. The department is reviewing what additional steps will be necessary to implement in order to get compliance on these notification procedures from County Treasurer staff. The new VicToRy System is set to require a new password at least every 90 days.

3. Application Change Management

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

- **MCS Application:** Two developers had the ability to check out code and promote any change developed to the production environment. The Department did not have a compensating control that would include reviewing the changes promoted to production to ensure they were proper.

- **VTR Application:** One of five changes tested lacked documentation to support that it had been approved.

- **VTR Application:** Three developers had the ability to check out code and promote any change developed to the production environment. The Department did not have a compensating control that would include reviewing the changes promoted to production to ensure they were proper.

- The Department used the Change Control Facility/Migration Management Facility (CCF/MMF) tool for tracking changes made to its mainframe applications. 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 to production.

NITC Technical Standards and Guidelines, Information Security Policy 8-202 (July 2017), "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 changes before implementation and ensure that accurate documentation is maintained.*

NITC Technical Standards and Guidelines, Information Security Policy 8-303(4) (July 2017), "Identification and authorization," 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, increased auditing and management supervision must be implemented. At a minimum, the audit of security must remain independent and segregated from the security function.*

Good internal controls require procedures to ensure that the Department's change management process is safeguarded by consistent change control standards and a segregation of duties.

Without such procedures, there is an increased risk that changes to an application might be made without specific management approvals, leading to possible data loss, compromised financial data integrity, or unintended system downtime.

A similar finding was noted during the previous audit.

> We recommend the Department implement an adequate segregation of duties to prevent a single user from performing an application change from start to finish. If segregation of duties is not possible, we recommend that compensating controls, such as reviewing changes quarterly, be documented. In addition, we recommend the Department ensure that the change management process be followed for all changes. Furthermore, we recommend the Department periodically review implementer changes and ensure service portal tickets are received for each change.

Department Response:

a. ***MCS Application*** *– The change management control process for the MCS application includes records of agendas and notes from the weekly review meetings, which are approved and signed by the Division Administrator and kept on file by the IT Division Administrator.*

b. ***VTR Application*** *– The new VicToRy System has a fully intergrade system to document any changes developed and deployed in the system.*

c. ***Change Control Facility/Migration Management Facility (CCF/MMF)*** *– This is the change management tool provided by the Chief Information Office. Department developers submit changes for applications on the mainframe to the CCF/MMF. The practice of the CIO is not to allow a change out of Implementer without their review for a change management ticket in the service portal. Currently all changes for the mainframe applications are being submitted and processed through CCF/MMF.*

4. NITC Information Security Policy

The Department did not complete all of the reports and assessments required by the NITC Information Security Policy, as follows:

- The Department did not have an Information Security Strategic Plan on file.
- The Department's System Security Plan did not include all the contents required by the NITC policy.
- Documentation was not on file to support completion of the most recent Department PCI data security control assessment.

NITC Standards and Guidelines, Information Security Policy 8-209 (July 2017), "State and agency security planning and reporting," states the following:

> *The following standard and recurring reports are required to be produced by the state information security officer and each agency information security officer; these reports will reflect the current and planned state of information security at the agency:*
>
> *(1) Information security strategic plan (section 8-210);*
>
> *(2) System security plan (section 8-211); and*
>
> *(3) Plan of action and milestones report (section 8-212).*

Sections 8-210 through Section 8-212 of the Information Security Policy outline the specific contents to be included in each report.

Good internal controls require procedures to ensure that the Department completes all of the reports and assessments required by the NITC Information Security Policy.

Without such procedures, there is an increased risk of noncompliance with the NITC Information Security Policy.

> We recommend the Department work with the State Information Security Officer to complete the reports required by the NITC Information Security Policy.

Department Response: The department is reviewing sections 8-210 to 8-212 of the NITC Standards and Guidelines and developing a plan for compliance.

* * * * *

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 management, 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.

Pat Reding, CPA, CFE
Assistant Deputy Auditor