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

September 11, 2020

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

Dear Ms. Lahm:

This letter is provided pursuant to AICPA Auditing Standards AU-C Section 265B.A17, which permits the early communication of audit findings due to their significance and the urgent need for corrective action. The audit work addressed herein was performed as part of the fiscal year ended June 30, 2020, Comprehensive Annual Financial Report (CAFR) audit. This communication is based on our audit procedures through June 30, 2020. Because we have not completed our audit of the fiscal year 2020 CAFR, additional matters may be identified and communicated in our final report.

In planning and performing our audit of the State's financial statements as of and for the year ended June 30, 2020, in accordance with auditing standards generally accepted in the United States of America, we considered the State's internal control over financial reporting (internal control) as a basis for designing the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, 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.

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 was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified.

We noted certain internal control or compliance matters related to the activities of the Nebraska Department of Motor Vehicles (Department), or other operational matters, which are presented below for your consideration. The following comments and recommendations, which have been discussed with the appropriate members of the agencies and their management, are intended to improve internal control or result in other operating efficiencies.

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. Where no response has been included, the Department declined to respond.

The following are our comments and recommendations for the year ended June 30, 2020.

1. Application Change Management

During testing of the Department's change management process for the Traffic Safety Information (TSI) application, we noted that 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, the individual reviewing changes to ensure no single user performed an application change from start to finish had the ability to check out code, develop a change, and move the change to production.

During testing of the Department's change management process for the Motor Carrier Services (MCS), we noted that 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. Additionally, only one person was trained to support the MCS application. As only one individual was able to provide support, there was an increased risk of services supported by the application being disrupted for a prolonged period.

Nebraska Information Technology Commission (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 a segregation of duties. Those same procedures should ensure also that more than one person is able to support the MCS application.

Without such procedures, there is an increased risk of not only changes to a mainframe application being made without specific management approval, leading to possible data loss, compromised financial data integrity, or unintended system downtime, but also the MCS system being vulnerable to prolonged disruption.

A similar finding was noted during the previous audit.

> We recommend the Department implement procedures to ensure an adequate segregation of duties to prevent a user from reviewing his or her own mainframe application changes. Those same procedures should provide also for training additional individuals to be able to support the MCS system.

2. NITC Information Security Policy

The Nebraska Information Technology Commission's (NITC) nine members are appointed by the Governor with the approval of the Legislature. Neb. Rev. Stat. § 86-516(6) (Reissue 2014) directs the NITC to do the following: "Adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel."

NITC Technical Standards and Guidelines, Information Security Policy 8-209 (July 2017), "State and agency security planning and reporting," requires or recommends State agencies to have an Information Security Plan, a System Security Plan, and a Plan of Action and Milestones Report on file. The NITC has established specific elements to be included in its Information Security Strategic Plan (8-210), System Security Plan (8-211), and Plan of Action and Milestones Report (8-212).

As a result, the Auditor of Public Accounts (APA) tested some of those key elements of the NITC Technical Standard and Guidelines to verify compliance by the Department. Though having various documents that contained some of the necessary elements, the Department lacked documentation to support that it met all required elements, as described below.

The APA noted the following requirements were not met regarding the Information Security Strategic Plan (8-210):

- Five-year projection and educated views of emerging threats and protections.

The APA noted the following requirements were not met regarding the System Security Plan (8-211):

- System operating status and description of the business process, including a description of the function and purpose of the systems included in the System Security Plan.
- A detailed diagram showing the flow of sensitive information including CONFIDENTIAL and RESTRICTED information.
- A review of security controls and assessment results that have been conducted within the past three years.

The Department also lacked a Plan of Action and Milestone report (8-212).

Additionally, documentation was not on file to support completion of the most recent Department Payment Card Industry (PCI) data security control assessment.

In addition to the NITC Technical Standards and Guidelines noted above, good internal controls require procedures to ensure that all elements of the Information Security Strategic Plan, System Security Plan, and Data Security Control Assessment are on file, as required by the NITC Information Security Policy.

Without such procedures, the Department lacks formal plans that describe fully the current controls in place for protecting information at a level commensurate with the sensitivity level of the Department's systems.

A similar finding was noted during the previous audit.

> We recommend the Department work with the State Information Security Officer to satisfy the requirements of the NITC Information Security Policy.

3. VicToRy Terminated Users

The Department uses the VicToRy application for vehicle registration and titling. During testing of terminated VicToRy users, we noted that 9 of 13 users did not have their access removed in a timely manner (three business days) after their termination date.

Employee	Termination Date	Access Removed	Business Days Between Termination and Access Removal	Cease Date per Security Request	Business Days Between Cease Date per Security Request and Access Removal
County 1	3/16/2020	4/16/2020	31	4/1/2020	11
County 2	2/21/2020	2/27/2020	4	2/27/2020	0
County 3	1/10/2020	5/11/2020	120	None Received	-
County 4	1/17/2020	5/18/2020	119	None Received	-
State 1	12/2/2019	1/7/2020	36	None Received	-
State 2	4/21/2020	5/26/2020	35	None Received	-
State 3	12/9/2019	12/27/2019	18	12/26/2019	1
State 4	12/20/2019	1/7/2020	14	None Received	-
State 5	10/28/2019	1/7/2020	71	None Received	-

The Cease Date per Security Request is the date the Department was notified by the County or the State agency that the employee had terminated and that the VicToRy access needed to be removed. Only three of nine users' access tested had the request made. For one of the three users, the access was not removed timely (within three days) after the Department was notified.

County Employees 3 and 4 were removed through the Department's periodic review of users who have not accessed VicToRy in over 90 days. The Department did not periodically verify the employment status of County employees to ensure the access was necessary. Instead, the Department removed all access after 90 days of inactivity.

For the five State employees whose access the Department did not remove in a timely manner, access to VicToRy was tied to access in the State's network. If the State agency had removed employee access to the State's network in a timely manner, the user would not have had access to VicToRy.

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.*

Good internal control requires procedures to ensure that terminated users have their access to VicToRy removed in a timely manner.

Without such procedures, there is an increased risk of unauthorized access to VicToRy.

A similar finding was noted during the previous audit.

> We recommend the Department implement procedures to ensure that terminated users have their VicToRy access removed in a timely manner. We also recommend the Department develop a procedure to review VicToRy user access, such as sending a listing of users to entities to determine if users have terminated and need their access removed.

* * * * * *

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.

Zachary Wells, CPA, CISA
Audit Manager