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 27, 2022

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 265.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, 2022, Annual Comprehensive Financial Report (ACFR) audit. This communication is based on our audit procedures through June 30, 2022. Because we have not completed our audit of the fiscal year 2022 ACFR, 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, 2022, 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, and, therefore, material weaknesses may exist that were not identified.

We noted certain internal control or compliance matters related to the activities of the 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. The Department declined to respond.

The following are our comments and recommendations for the year ended June 30, 2022.

1. Motor Carrier Services (MCS) Control Issues

The Department uses the Motor Carrier Services (MCS) system to calculate and track amounts due to Nebraska and other states for the International Registration Plan (IRP), the Unified Carrier Registration (UCR) program registrations, and the International Fuel Tax Agreement (IFTA) collections. During testing of the Department's change management process for the MCS system, 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, this same person was the only individual trained to support MCS. As only one individual can provide support, there is 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 MCS.

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. Furthermore, relying on one individual's knowledge for MCS support leaves the system vulnerable to disruption for a prolonged period.

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 application changes. Those same procedures should provide also for training additional individuals to be able to support the MCS system.

2. Traffic Safety Information System (TSI) Change Management Process

The Department used the Traffic Safety Information System (TSI) to issue driver's licenses and other permits. The following issues were noted during testing of the TSI change management process:

- For 8 of 19 changes tested, the Auditor of Public Accounts (APA) noted an absence of documentation to support that the change was tested before moving to production. Per the Department, testing was completed, and each change request documented the "test plan" that was used for testing changes. However, due to how the change request tickets were archived, no documentation could be provided to support that testing was completed for each change.

- For 2 of 19 changes tested, no change request to support the system change was on file.

- For 8 of 19 changes tested, there was no documentation that management approved the request before implementing the change to production.

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.*
>
> * * * *
>
> *All IT infrastructure and application development changes are required to follow a change management process to ensure the change is approved for release and does not unknowingly add security risks to the state's environment.*

A good internal control plan requires procedures to ensure that changes to TSI undergo documented testing, prior to promotion to production, to ensure that those changes are in accordance with management's intentions.

Without such procedures, there is an increased risk of unauthorized, and potentially harmful, changes to TSI.

> We recommend the Department implement procedures to ensure documentation is maintained to support the result of testing changes prior to changes being promoted to production. We also recommend the Department strengthen procedures to ensure change requests are completed and approved by management for all changes made.

3. VicToRy Terminated Users

The Department utilizes the VicToRy system for recording of vehicle registrations and titles, including the associated collections for these registrations and titles. During testing of terminated users, the following was noted:

- For 5 of 11 terminated VicToRy users tested, access was not removed in a timely manner (3 business days) after the employee was terminated, ranging from 7 to 71 days after the termination date. One of these terminated users signed into VicToRy nine days after her termination date.

- For 1 of 11 terminated VicToRy users tested, access was not removed in a timely manner (3 business days) after the cease date per the security request. Access for this user was removed 32 days after the cease date in the security request.

Good internal controls require procedures to ensure that access to VicToRy is removed in a timely manner after the user's termination date.

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

> We recommend the Department implement procedures to ensure that user access to VicToRy is removed promptly upon employee termination.

4. Nebraska Information Technology Commission (NITC) Information Security Policy

The nine members of the Nebraska Information Technology Commission's (NITC) 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 2021), "Agency security planning and reporting," requires or recommends State agencies to have an Information Security Strategic Plan and a System Security Plan on file. The NITC has established specific elements to be included in its Information Security Strategic Plan (8-210) and System Security Plan (8-211). These items are required if the agency has Federal data exchange agreements. Otherwise, these are considered guidelines and best practices by the NITC per Policy 8-209.

Furthermore, NITC Technical Standards and Guidelines, Information Security Policy 8-806 (July 2017), "Security deficiencies," requires security deficiencies identified to be documented in a report tracking the deficiencies' "mitigation, remediation, or approved risk acceptance."

As a result, the APA tested the Department's compliance with some of the key elements of those NITC Technical Standards and Guidelines. 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 failures to carry out the recommendations contained in NITC Policy 8-211 (July 2021), "System security plan":

- A detailed diagram showing the flow of information was lacking.
- No review of security controls and assessment results that have been conducted within the past three years appears to have been performed.

We noted that the Department lacked documentation (including the Department's mitigation, remediation, or approved risk acceptance) of all security deficiencies reported or identified in any security review, scan assessment, analysis, or IT audit, as required by NITC Policy 8-806.

Good internal control requires procedures to ensure compliance with NITC Technical Standards and Guidelines.

Without such procedures, there is an increased risk of the Department lacking formal plans that describe fully the current controls in place for protection of information at a level commensurate with the sensitivity level of the Department's systems.

> We recommend the Department formally document compliance with these guidelines or requirements, specifically documenting a risk assessment or review. Furthermore, we recommend the Department document the "mitigation, remediation, or approved risk acceptance" of any security deficiencies identified in a risk assessment, review, or information system audit.

* * * * *

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 interim 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 suitable for any other purpose. However, this communication is a matter of public record, and its distribution is not limited.

Zachary Wells, CPA, CISA
Assistant Deputy Auditor