



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 25, 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, 2018, 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 January 4, 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. This comment and recommendation, which has been discussed with the appropriate members of the Department's management, is 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 September 27, 2018.

Draft copies of this letter were furnished to the Department to provide management with an opportunity to review and to respond to the comment and recommendation contained herein. The Department declined to respond.

The following is our comment and recommendation for the year ended June 30, 2018.

1. **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 segregation of duties issues:

- **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.
- **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.

A similar finding was noted during the previous audit.

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-202 (July 2017), 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.

NITC Standards and Guidelines, Information Security Policy 8-303 (July 2017), Identification and Authorization, Section 4, 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.

NITC Standards and Guidelines, Information Security Policy 8-502 (July 2017), Minimum User Account Configuration, states the following:

- (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.*
- (2) Administrator level access is privileged and must be restricted to authorized IT personnel only. All privileged access accounts are subject to additional security, including multi-factor authentication, and enhanced auditing and logging of activity.*
- (3) Local accounts must be disabled unless required for business purposes, and in those cases, use of these accounts must be approved, tightly controlled, and monitored. All use of local accounts are [sic] required to be associated with an individual user.*

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.

We recommend the Department implement an adequate segregation of duties to prevent a single user from performing an application change from start to finish. We recommend the Department develop and implement a formalized change management process for MCS, VTR, and TSI applications. The process should include documented change requests, testing procedures, management approval, and implementation into production.

* * * * *

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
Assistant Deputy Auditor