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 24, 2017

Rhonda Lahm, Director
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, 2016, 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 15, 2016. 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 Department of Motor Vehicles (Department) or other operational matters that are presented below for your consideration. The 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.

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 the Department's internal control that we consider to be material weaknesses or significant deficiencies. However, material weaknesses or significant deficiencies may exist that were not 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. The Department declined to respond.

The following are our comments and recommendations for the year ended June 30, 2016.

1. Application Support

The Department uses multiple computer applications to meet its statutory responsibilities. They include the Vehicle Titling and Registration (VTR) application, which provides an overall system to be utilized by the counties in vehicle titling and registration, and the Motor Carrier Services (MCS) application, which supports the International Registration Program (IRP), the International Fuel Tax Agreement (IFTA) Program, and the Unified Carrier Registration (UCR) Program.

The programming support for the VTR and MCS applications consisted of one individual (for each application) with both the business knowledge and the programming skill set required to support the applications. The Department noted that the business knowledge of the applications specified above could take years for another individual to acquire. The MCS programmer is a contractual employee. The Department is currently working on a project to modernize and replace VTR and MCS operations and systems, which would require a less specialized programming skill set. However, the Department currently has a limited backup plan should the individuals currently supporting the applications become unavailable:

- **VTR Application:** The Department is in the process of finalizing a Memorandum of Understanding with the Court Administrator's Office to provide backup support for the VTR application. The backup support, if agreed upon, would not be available until the new VTR system is in production. Once operating on the new VTR system, the Department plans to determine workload and backup support requirements needed to adequately support the VTR application.

- **MCS Application:** The Department has been in contact with the Office of the Chief Information Officer (OCIO) regarding backup application support. In the event that additional or replacement application developers are needed to support the MCS application, the Department will utilize the existing Covendis contract to add or replace resources. This contract provides IT personnel to staff temporary IT positions. Once operating on the new MCS system, the Department will determine workload and backup support requirements needed to adequately support the MCS application.

A similar finding has been reported in previous audits.

Nebraska Information Technology Commission (NITC) Standards & Guidelines, Information Technology Disaster Recovery Plan Standard 8-201 (August 2006), Section 1, states the following, in relevant part:

> *Each agency must have an Information Technology Disaster Recovery Plan that supports the resumption and continuity of computer systems and services in the event of a disaster. The plan will cover processes, procedures, and provide contingencies to restore operations of critical systems and services as prioritized by each agency . . . .*

The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency. The following elements, at a minimum, must be included:

- *Identification of critical computer systems and services to the agency's mission and business functions.*
- *Critical systems and services preservation processes and offsite storage strategy and methods to protect storage media . . . .*
- *Annual plan review, revision, and approval process.*

Additionally, NITC Standards & Guidelines, Information Technology Disaster Recovery Plan Standard 8-201, Section 5.2, Agency and Institutional Heads, states the following:

The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs, consistent with this standard. The authority may delegate this responsibility but delegation does not remove the accountability.

When only one person is trained to support an application, there is an increased risk services supported by the application may be disrupted for a prolonged period of time.

We recommend the Department evaluate the risk associated with relying on one individual to provide application support. We also recommend the Department consider training additional staff to support the VTR and MCS applications.

2. VTR and MCS Application Users

The Department indicated it conducted a full user review of the VTR and MCS applications in August of 2015; however, it did not provide documentation to support this review. Additionally, the Department has not established procedures to perform a full user review on at least an annual basis.

A similar finding was noted during the previous audit.

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.7.2, User Account Management, states 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.

When user access to applications is not periodically reviewed, it creates the opportunity for inappropriate access to State resources.

We recommend the Department implement procedures to review user access to its applications on an annual basis.

3. Application Change Management

The Department's change management process was informal for the MCS, VTR, and Traffic Safety Information (TSI) applications. We also noted the following:

- **MCS Application** – One developer was responsible for the change management process for the MCS application. This developer was able to perform all change management functions and could develop a change and move it to production without involving anyone else. The developer met weekly with management to discuss all changes that were in development, testing, or completed, as noted on a project list. This project list was then signed by the Department MCS Administrator to indicate review and approval of the changes discussed. Though a documented review of the project list is being performed, there is risk that not all changes made by the developer are included on the project list.

- **VTR Application** – The Department uses the Implementer tool to track and implement changes to the VTR application. Users are set up in Implementer with access to various environments and functions. This includes the ability to check out and move code from one environment to a different environment. We noted six user IDs, two at the Department and four at the OCIO, had move and checkout access to the VTR development, test, and production environments. Three of the four OCIO employees have not only this access but also access to push changes out to the county AS/400s using the System AS/400.

  During testing of changes made to the VTR application for the fiscal year ended June 30, 2016, we also noted that seven of ten changes did not have adequate documentation of who developed, tested, approved, and moved the change to production. We noted that two of the seven changes did have documentation that the Motor Vehicle Titles & Registration Administrator was aware of the changes; however, there was not documentation of a second individual involved in the testing or migration of the changes.

- **TSI Application** – The Department uses the Implementer tool to track and implement changes to the TSI application. We noted five user IDs, two at the Department and three at the OCIO, had move and checkout access to the TSI development, test, and production environments. All three of the OCIO employees have not only this access but also have access to push changes out to the county AS/400s using the System AS/400.

  The Department uses the CCF/MMF tool for tracking changes made to the TSI application. During a review of access to the CCF/MMF tool, six 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.

NITC Standards & Guidelines, Information Security Policy 8-101, 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, 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.

Without proper and consistent change control standards and 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 an increased risk that a change could be developed and moved into production without separate review and approval.

We recommend the Department develop and implement a formalized change management process for the 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 without a secondary review and approval.

4. Security Settings

Both the State AS/400 and the county AS/400s on which the VTR application resides have no timeout setting, outside of the hours of 6:00 PM - 7:00 PM, when it is set at 30 minutes. Thus, this timeout setting would apply to all State and county employees who have access to this application. The Department indicated having no timeout setting on the AS/400s used by the counties is a matter of operational efficiency. Additionally, as the Supreme Court's Judicial User System to Improve Court Efficiency (JUSTICE) application also resides on the county AS/400s, and the timeout setting can only be changed by AS/400 (not by application), changing the county AS/400s' setting would impact not only VTR users but also JUSTICE users.

The AS/400 on which the MCS application resides has no timeout setting outside of the hours of 6:00 PM - 7:00 PM and 2:00 AM - 3:00 AM, when it is set at 30 minutes.

A similar finding was noted during the previous audit.

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.5.4, Clear Screen, states the following:

> *To prevent unauthorized access to information, agencies will implement automated techniques or controls to require authentication or re-authentication after a predetermined period of inactivity for desk tops, laptops, PDA's and any other computer systems where authentication is required. These controls may include such techniques as password protection screen savers, automated logoff processes, or re-authentication after a set time out period.*

A good internal control plan includes utilizing re-authentication rules that require users to comply with NITC standards.

An excessive period of inactivity between required re-authentication increases the risk of an unauthorized user gaining access to confidential information and key financial data.

We recommended the Department work with the Supreme Court and the OCIO to implement a re-authentication setting for the AS/400s. We recommend a timeout setting of 30 minutes or less.

* * * * *

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