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 29, 2016

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

Dear Mrs. 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, 2015, 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 17, 2015. 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 (Agency) 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 Agency'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 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 Agency to provide management with an opportunity to review and to respond to the comments and recommendations contained herein. The Agency declined to respond.

The following are our comments and recommendations for the year ended June 30, 2015.

1. Application Support

Nebraska Information Technology Commission (NITC) Standards & Guidelines, Information Technology Disaster Recovery Plan Standard 8-201, 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.*

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

The programming support for the MCS and VTR applications consisted of one individual with both the business knowledge and the programming skill set required to support the applications. The MCS programmer is a contractual employee. The Agency has a limited backup plan should the contractual programmer become unavailable. According to the Agency IT manager, assistance from the Department of Administrative Services Office of the Chief Information Officer (OCIO), and possibly from former Agency employees, would be utilized if the individuals were to become unavailable. The Agency IT manager also noted that the business knowledge of the applications noted above could take years to acquire. The Agency IT manager acknowledged these risks and explained that the Agency has sought to mitigate them by creating

a strategic business plan that outlines future projects and will define the specific needs and skills required for the application development staff for all functional areas.

A similar finding has been reported in previous audits.

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

2. Application Change Management

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.*

The Agency uses multiple computer applications to meet its statutory responsibilities. Among those applications are the following:

- The MCS application, which supports the IRP, IFTA program, and the UCR program.
- The VTR application, which is utilized by the counties in vehicle titling and registration.
- The Traffic Safety Information (TSI) application, which is utilized by the counties to create, maintain, and update driver records.

The Agency's change management process was informal for these applications. We also noted the following for the above applications:

- **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. Beginning in December 2014, this project list was then signed by the Agency MCS Administrator to indicate review and approval of the changes discussed.

- **VTR Application** – Implementer is the change management tool used for 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 an environment to a different environment. Six user IDs, two at the Agency and four at the OCIO, had move and checkout access to the VTR development, test, and production environments, allowing them to check out code, make changes, and move the changes to production through Implementer. Three user IDs, all OCIO employees, of the six also had the ability to promote changes to be sent out to the counties.

  During our review of the VTR change management process, we noted the Agency maintained a folder that included a project schedule, test plans, and various goal dates.

  During testing of changes made to the VTR application for the fiscal year ended June 30, 2015, we also noted that 7 of 10 changes did not have adequate documentation. Changes made prior to March 2015 did not have adequate documentation of who developed, tested, approved, and moved a change to production. During March 2015, the Agency began documenting the change management process for VTR changes through email discussions among the agency director, program administrator, and IT staff.

- **TSI Application** – Two developers had the ability to check out TSI code (which relates to the interface between VTR and TSI), make changes, and ultimately promote the change to the point where the OCIO moved the changes into production. In addition, three developers had the ability to check out mainframe code, develop changes, and approve the change for movement into the production environment. These developers used the automated Change Control Facility/Migration Management Facility (CCF/MMF) tool for this process.

  In addition, we noted through discussion with IT staff that changes to the TSI application are explained in the program specifications; however, the approval of the test results and the approval to move the application change into production is typically verbal.

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.

We recommend the Agency develop and implement a formalized change management process for 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 Agency continue to use the process implemented in March 2015 for VTR application changes. Finally, we recommend the Agency implement an adequate segregation of duties to prevent a single user from checking out code, developing, and promoting changes to the point where the OCIO moves the change to production.

3. VTR and MCS Application Users

NITC Standards and Guidelines, Information Security Policy 8-101, 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.*

The Agency did not perform an annual review of users with access to the MCS and VTR applications. During our review of users with AS/400 MCS access, we noted a substantial decrease in the number of users from 379 users in the prior year to 148 users in the current year. We inquired of Agency IT staff regarding the process for reviewing user access to Agency applications and to determine when users were deleted. The Agency indicated the removal of users occurred in conjunction with a request for user information. The Agency IT staff further noted that access to MCS and VTR applications is reviewed periodically, but a full review had not been initiated in the past year.

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

We recommend the Agency implement procedures to review annually user access to its applications.

4. Security Settings

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.

The MCS and VTR applications reside on an AS/400 computer at the OCIO. According to the Agency and the OCIO, the AS/400 on which the MCS application resides has no timeout setting, while the AS/400 on which the VTR application resides has no timeout setting outside of the hours of 6:00PM-7:00PM, when it is set at 30 minutes. The VTR setting would include all State and county employees who have access to this application. The Agency indicated having no timeout setting on the AS/400s used by the counties is a matter of operational efficiency.

In addition, previous audits have noted that the Supreme Court's Judicial User System to Improve Court Efficiency (JUSTICE) application, which is used by the county and district courts to record all financial and case activity, also resides on the same AS/400s. Thus, its security setting is the same as above.

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 Agency work with the Supreme Court and the OCIO to determine if a re-authentication setting for the Agency application and applicable JUSTICE application could be set at a more reasonable level, such as 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 Agency 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 Agency.

This communication is intended solely for the information and use of the Agency, the Governor and State Legislature, others within the Agency, 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.

Don Dunlap

Don Dunlap, CPA
Assistant Deputy Auditor