NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

Mike.Foley@nebraska.gov
PO Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
www.auditors.nebraska.gov

December 16, 2014

Rhonda Lahm, Director
Nebraska Department of Motor Vehicles
301 Centennial Mall South, 1st Floor
Lincoln, Nebraska 68509-5026

Dear Mrs. Lahm:

We have audited the basic financial statements of the State of Nebraska (State) as of and for the year ended June 30, 2014, 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, and have issued our report thereon dated December 16, 2014. 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 for the purpose of expressing our opinions on the basic 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 (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 and, therefore, 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. All formal responses received have been incorporated into this letter. Responses have been objectively evaluated and recognized, as appropriate, in the letter. Responses that indicate corrective action has been taken were not verified at this time, but they will be verified in the next audit.

The following are our comments and recommendations for the year ended June 30, 2014.

1. Application Support

NITC Standards & Guidelines, Information Technology Disaster Recovery Plan Standard 8-201, Section 1, states, in 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 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 Motor Carrier Services (MCS) application tracks motor carrier registration fees and taxes. It supports the International Registration Program (IRP), International Fuel Tax Agreement (IFTA) program, and the Unified Carrier Registration (UCR) program.

The Vehicle Titling and Registration (VTR) application provides an overall system to be utilized by the counties in vehicle titling and registration.

Both the MCS and VTR applications were supported by only one individual with both the business knowledge and the programming skill set required to support the application. The Agency had no backup plan if the programmer became unavailable.

A similar comment was noted during the previous three 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 risks associated with relying on one individual to provide application support and consider training or hiring additional staff to support the MCS and VTR applications.

Agency Response: The DMV is aware of the risk associated with not having duplicative staff for each functional area. To begin mitigating this risk, the DMV has developed a strategic business plan that outlines future projects and defines the specific need and skills required for the additional application development staff. The first definitive step will be the hiring of an additional VTR developer in January of 2017 as part of the Nebraska Systems Update and Modernization project. The DMV will continue to evaluate the specific needs of all divisions within the Department and will develop the skills of existing staff wherever possible.

2. Application Change Management

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.9.11, Change Control Management, states:

> *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:

> *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 Traffic Safety Information (TSI) application provides an overall system to be utilized by the counties to create, maintain, and update driver records.

The Agency's change management process was informal. The Agency did not maintain supporting documentation for database changes. We also noted the following:

- Three developers had the ability to check out VTR code, make changes, and ultimately promote the change to the point where the Office of the Chief Information Officer (OCIO) moved the changes into production.

- Two developers had the ability to check out TSI code, make changes, and ultimately promote the change to the point where the OCIO moved the changes into production.

- Three developers had the ability to check out mainframe code, develop changes, and approve the change for movement into the production environment. The developers had access to the automated Change Control Facility/Migration Management Facility (CCF/MMF) tool.

A similar comment was noted during the previous audit.

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 down time.

> We recommend the Agency develop and implement a formalized change management process for MCS, VTR, and TSI applications. The process should include documented change requests, testing procedures, and management approval to implement the change into production. 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.

Agency Response: The organizational structure and interactions of the IT Division within the DMV have been developed to maximize resources and operational efficiency while mitigating the associated risks. Historically, the DMV IT Division has worked directly with Division Administrators within the Department. All database and application changes are performed only at the request of the Division Administrator that owns the data and process. All database and application changes are tested and approved by the authorized division prior to implementation. Even though this process has functioned efficiently and without significant failure, the DMV will be reviewing existing procedures and work towards developing a more formal process that is expected to require written requests for changes and approval of changes prior to implementation into a production environment.

The DMV will evaluate all opportunities to further segregate the duties of its IT staff and make all reasonable operational changes.

* * * * *

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.

Philip Olsen, CPA, CISA
Audit Manager