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

Matt Blomstedt, Commissioner
Nebraska Department of Education
301 Centennial Mall South
P.O. Box 94987
Lincoln, NE 68509-4987

Dear Commissioner Blomstedt:

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 Education (Department) 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 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 and, therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as discussed below, we identified a certain deficiency in the Department's internal control that we consider to be a significant deficiency.

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. We did not identify any deficiencies in internal control that we consider to be material weaknesses.

A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider Comment Number 1 (Average Daily Membership Verification) to be a significant deficiency.

This comment will also be reported in the State of Nebraska's Statewide Single Audit Report Schedule of Findings and Questioned Costs.

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. 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, 2016.

1. Average Daily Membership Verification

During our review of State Aid, we noted all five audit firms tested did not appear to perform adequate compliance testing of school districts' Average Daily Membership (ADM) to provide sufficient assurance that amounts reported to the Department were correct. The testing of ADM compliance by district auditors was also inconsistent.

ADM is an integral figure used within the State Aid formula to determine the amount of aid provided to school districts.

The Department distributed $973,036,624 of State Aid in the State fiscal year ended June 30, 2016.

The Department's administrative rules and regulations, Title 92 Nebraska Administrative Code (NAC) Chapter 1-003.03, state the following, in relevant part:

> *The audit shall include tests for compliance with the calculation of Average Daily Membership reported on the Annual Statistical Summary Report . . . .*

A good internal control plan requires procedures to ensure adequate reviews of ADM are performed.

Not ensuring the accuracy of ADM submitted by school districts increases the risk of the State Aid distribution being incorrect.

> We recommend the Department ensure that school district auditors perform adequate compliance testing of ADM. At a minimum, such testing should include the tracing of ADM to supporting documentation, the recalculation of ADM, verification of ADM reported to the Department, and the documentation of all testing procedures performed.

Department Response: As noted in the finding, Rule 1 does require independent school district auditors to test average daily membership (ADM). Per discussion with independent auditors who are performing school district audits, they are testing ADM but there have been no findings related to Membership/Attendance and thus no documentation of their testing is noted in the audit reports per auditing standards.

School districts submit attendance and membership information to the state and then average daily membership is calculated by the Department based on the submitted data. For schools to inflate their membership they would have to create fake students with unique IDs. These students would then need to have attendance records kept; test scores entered and would be on a list that teachers and others staff would review. The Department also performs analytical tests on membership information to confirm that the membership and attendance information submitted is reasonable.

Corrective Action Plan: The Department has worked with the Nebraska Society of CPA's to develop a new form which outlines the tests independent auditors performed on membership and attendance and notes if the information submitted to the Department was accurate. The department now requires confirmation of membership and attendance testing to be submitted along with the audit before considering the audit submission complete.

2. Information Technology (IT) Risk Assessment

We noted the Department prepared an IT risk assessment report; however, it lacked application-specific risk information. The Department has multiple applications, which may have different levels of risk.

A similar finding was noted during the previous audit.

NITC Standards and Guidelines, Information Security Policy 8-101 (December 10, 2013), Section 4.5.1, Physical Security Perimeter, states, in relevant part, the following:

> *Agencies will perform a periodic threat and risk assessment to determine the security risks to facilities that contain State information . . . .*

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.9.3, Risk Assessment, states, in relevant part, the following:

> *Security requirements and controls must reflect the value of the information involved, and the potential damage that might result from a failure or absence of security measures . . . . The framework for analyzing the security requirements and identifying controls to meet them is associated with a risk assessment, which must be performed by the data owner(s) and Agency management. A process must be established and implemented for each application to:*

- *address the business risks and develop a data classification profile to help to understand the risks;*
- *identify security measures based on the criticality and data sensitivity and protection requirements;*
- *identify and implement specific controls based on security requirements and technical architecture;*
- *implement a method to test the effectiveness of the security controls; and*
- *identify processes and standards to support changes, ongoing management and to measure compliance.*

A good internal control plan requires procedures to ensure that an IT risk assessment is completed and updated periodically. Those procedures should require the assessment to address application-specific risk information.

Without such procedures, there is an increased risk that an application's threats will not be identified. This increases the risk of preventable security vulnerability and threat exploitation, causing such issues as downtime, loss of productivity, unauthorized access, compromise of confidential information or data integrity, or interference with other State or Federal systems.

> We recommend the Department implement procedures to ensure the periodic performance of an IT risk assessment that addresses application-specific risk information.

Department Response: The Department recognizes the importance of the IT risk assessment to ensure protection from security vulnerability and threat exploitation, causing such issues as downtime, loss of productivity, unauthorized access, compromise of confidential information or data integrity, or interference with other State or Federal systems. To that end, the Department is undertaking multiple steps to expand the IT security audit procedures. The Department is confident that through accomplishing these steps and the related tasks that we will be in a better position to identify and mitigate the risks associated with the applications developed and several additional areas of security will be enhanced as well.

3. Developer Access to Production Environment

One Disability Determination System (DDS) application developer and one DDS contracted developer at the Department had full access to the production environment.

Two QE2 (Vocational Rehabilitation System) application developers had access to develop code and move changes into production.

A similar finding was noted during the previous audit.

Nebraska Information Technology Commission (NITC) Standards and 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.*

NITC Standards and 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 application as well as systems software used to maintain operating systems, network software, hardware changes, etc.*

Good internal controls require procedures to ensure application changes are approved and documented. This includes implementing a segregation of duties in the change management process when migrating changes to production environments. If a segregation of duties cannot be maintained due to staff size, compensating controls should be implemented, including the review of audit logs, code changes, or automatic notifications by someone other than the developer(s) to identify all changes made to the production environment.

Without such controls, application developers with access to the database and the production environments will have the ability to circumvent the standard change control process and implement modifications that may be inconsistent with management's intentions and could result in unauthorized changes to data.

> We recommend the Department implement procedures to ensure the approval and documentation of application changes. Additionally, a proper segregation of duties should be implemented in the change management process when migrating changes to production environments. Absent such a segregation of duties, we recommend implementing appropriate compensating controls.

Department Response: All changes to production are now documented in Redmine. Documentation includes who made the request, programming changes that are made as a result of the request, who tested the changes, and who approved the push to production. In 2016 the VR IT Department set up new code versioning infrastructure as a part of VR's migration to OCIO datacenter and virtualization strategy. This required coordinating many pieces internally and with OCIO (procuring and setting up a new virtual host, getting access to the OCIO datacenter, migrating the host, creating the new gitlab repository, opening network firewalls, testing code provisioning, creating backups, etc.) Our inhouse code repository (gitlab) was set up at the end of August 2016. The IT Support Analyst Lead was set up and trained to merge approved code (approved at QE2 Change Committee meetings) 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
Audit Manager