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 18, 2014

Matthew Blomstedt, Commissioner of Education
Department of Education
301 Centennial Mall South, 6th Floor
Lincoln, Nebraska 68509-5026

Dear Mr. Blomstedt:

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 Education (Agency) 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 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. However, as discussed below, we identified a certain deficiency in 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 (Incorrect Accrual Information) 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 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 will be verified in the next audit.

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

1. Incorrect Accrual Information

The Department of Administrative Services State Accounting Division (State Accounting) prepares the State Comprehensive Annual Financial Report (CAFR) and requires all State agencies to determine and report payable and receivable amounts at the end of the fiscal year on an accrual response form. A good internal control plan requires agencies to have procedures for the reporting of accurate financial information to State Accounting.

We noted that three of six accruals tested were not properly reported to State Accounting for inclusion in the financial statements. For one accrual, the incorrect amount was included on the response form for an overstatement of $20,885,605. The other two accruals were not properly calculated, causing the accruals to be overstated by $1,597,949, and $74,199. The total overstatement was $22,557,753. Corrections were sent to State Accounting.

Without proper controls to ensure the accuracy of amounts reported to State Accounting, there is an increased risk of financial statement errors not being detected and corrected in a timely manner.

> We recommend the Agency implement procedures to ensure amounts reported are complete and accurate.

Agency Response: NDE has reviewed and updated its procedures to ensure all accruals submitted to State Accounting in the future are reviewed for completeness and accuracy.

2. Application Change Management and User Access

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

> *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.*

A sound business practice includes maintaining documentation to support who requested, developed, tested, and approved a change in order for the change to be promoted to production.

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, states:

> *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.*

A good internal control plan includes a process to ensure terminated users' access is removed in a timely manner.

The QE2 application is utilized by Vocational Rehabilitation staff to track all expenses paid to assist physically and/or mentally disabled persons in locating jobs. It includes aid to complete school, assistance to purchase dress clothes, assistance to set up interviews, etc.

For 3 of 10 QE2 application changes tested, there was not sufficient documentation to determine if the changes had been tested prior to being moved to the production environment.

For 2 of 4 terminated QE2 users tested, access was not removed in a timely manner. One employee's access was disabled 19 days after termination. The access of one user, who terminated from an external entity, was removed 90 days after termination.

When changes are not properly documented, there is an increased risk a change could be developed and promoted to production that is not in agreement with management's intentions. When access is not terminated timely, it creates the opportunity for inappropriate access to State resources. Such access may violate Federal laws regarding privacy issues.

We recommend the Agency implement procedures to adequately document all steps of a change to applications, including when and by whom the change was requested, tested, approved, and promoted to production. We also recommend application owners review user access on a periodic basis to ensure access is appropriate. Additionally, a formalized process to remove access to applications and networks should be established and followed, including communication with external parties on the importance of notifying the State of terminations, so access can be removed in a timely manner.

Agency Response: The processes and procedures recently developed through the Project Management Office (PMO) provide Project Management Book of Knowledge (PMBoK) standards in line with the NITC standards in managing changes and change logs. In addition, an internal team is finalizing a set of standards associated with application development, documentation, and other topics and will implement the aspects of change management as part of an addendum to these standards.

A review process of users with access continues to be finely tuned and supported through the work of the Network team oversight.

3. GMS Password Settings

NITC Standards and Guidelines, Password Standard 8-301, states, in part:

> *All employees and contractors of the State of Nebraska shall use a password that follows at least a confidential level of authentication when logging into a state network or application . . . . A password used to access confidential information must follow the password complexity rules outlined in section 1.2 and must contain the following additional requirement: Expire after 90 days.*

The Grants Management System (GMS) is used by outside users to apply for grants and by the Agency to approve and process disbursements of grants.

Passwords for school district users, used to access the GMS portal, did not have a change requirement. A similar finding was noted during the prior audit.

Without proper password settings, there is an increased risk for unauthorized access to the GMS application.

We recommend the Agency implement password settings that are in compliance with NITC standards and guidelines.

Agency Response: Changes have been made to the GMS system access through the NDE Portal related to passwords effective November 1, 2014.

4. Agency Risk Assessment

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.5.1, Physical Security Perimeter, states, in part:

> *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:

> *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 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 a risk assessment to be completed and updated periodically.

The Agency performed some risk assessment activities but lacked a formalized risk assessment plan for all applications within the Agency. A similar finding was noted during the prior audit.

When a comprehensive risk assessment is not performed, there is an increased risk that security vulnerabilities, which might have been prevented or monitored, could be exploited. This could cause downtime, loss of productivity, unauthorized access, or interference with State and/or Federal systems.

> We recommend the Agency complete a full risk assessment on a periodic basis.

Agency Response: NDE will be working to complete a formal Risk assessment per NITC standards during the 2014-2015 fiscal year. Progress continues to be made related to identifying the severity and confidentiality levels of the data with the program data owners and data stewards. In addition, the focus data governance and data access and use training among staff at NDE continue to be enhanced. A complete security risk assessment will become a standard annual process.

5. Application Developer Access to Production Environment

NITC Standards and 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.*

A good internal control plan includes restricting access to information resources based upon job responsibilities to help enforce a proper segregation of duties and reduce the risk of unauthorized system access. Programmers should generally be limited to accessing only the information specifically required to complete their assigned systems development projects, as well as be expressly prohibited from altering production data and production software.

The Disability Determination System (DDS) serves as a customer resource manager and information tracking system for payments to medical practitioners for information they provide to the social security administration pertaining to pending disability claims.

Two DDS application developers and one DDS contract developer had full access to the production environment. A similar finding was noted during the prior audit.

Application developers with access to the database and the production environment have the ability to circumvent the standard change control process and implement modifications that may be inconsistent with management's intentions, which could result in unauthorized changes to data.

> We recommend the Agency implement controls 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, we recommend implementing compensating controls. Compensating controls may include reviewing audit logs, code changes, or automatic notifications by someone other than the developer(s) to identify all changes made to the production environment.

* * * * *

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.

Pat Reding

Pat Reding, CPA, CFE
Assistant Deputy Auditor