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
auditors.nebraska.gov

September 11, 2020

Matt Blomstedt, Commissioner
Nebraska Department of Education
301 Centennial Mall South
Lincoln, Nebraska 68509

Dear Commissioner Blomstedt:

This letter is provided pursuant to AICPA Auditing Standards AU-C Section 265B.A17, which permits the early communication of audit findings due to their significance and the urgent need for corrective action. The audit work addressed herein was performed as part of the fiscal year ended June 30, 2020, Comprehensive Annual Financial Report (CAFR) audit. This communication is based on our audit procedures through June 30, 2020. Because we have not completed our audit of the fiscal year 2020 CAFR, additional matters may be identified and communicated in our final report.

In planning and performing our audit of the State's financial statements as of and for the year ended June 30, 2020, in accordance with auditing standards generally accepted in the United States of America, we considered the State's internal control over financial reporting (internal control) as a basis for designing the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, 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.

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.

Our consideration of internal control was for the limited purpose described in the preceding 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.

We noted certain internal control or compliance matters related to the activities of the Nebraska Department of Education (Department), or other operational matters, which are presented below for your consideration. The following comments and recommendations, which have been discussed with the appropriate members of the agencies and their management, are intended to improve internal control or result in other operating efficiencies.

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 were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, the auditor does not express an opinion on them. 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, 2020.

1. User Access Issues

During the Auditor of Public Accounts' (APA) review of users with access to the Child Nutrition Program (CNP), Vocational Rehabilitation's QE2, and the Grants Management System (GMS) applications, we noted users who were either granted unnecessary access or did not have their access removed in a timely manner (three business days).

CNP is used by the Department to administer the National School Lunch Program, Summer Food Service Program, Child and Adult Care Food Program, and the Commodity Program, including processing program claims and applications. During testing, we noted the following:

- Two employees had access to a generic ID that provided unrestricted access to CNP. The Department lacked procedures for formally tracking which employee had used the ID.
- One employee terminated employment with the State on February 18, 2020; however, he was still listed as an active user on the CNP access report provided to the APA on April 13, 2020.
- One of 19 CNP users tested had access that was not required to perform her job duties. The employee had not accessed CNP since May 2019; nevertheless, when this concern was brought to the Department's attention, the access was removed. This user had access to approve applications to the School Nutrition Program.

QE2 is used by the Department to track all expenses paid to assist physically or mentally disabled persons with locating jobs. During testing, we noted the following:

- Two of three terminated users tested did not have access removed in a timely manner. According to Vocational Rehabilitation (VR), the normal process was to change terminated employees' passwords so they could no longer log into QE2, while reassigning those terminated users' cases. However, VR did not have documentation to support when the passwords were changed for the two employees. The two employees were not deactivated from QE2 until 15 business days after termination.
- Two employees terminated employment on March 16, 2020, and March 30, 2020, respectively. Both individuals still had access to QE2 as of April 17, 2020. One employee had elevated access that allowed unrestricted access to the application.

GMS is used by the Department for processing grant applications and grant payments for various State and Federal grants. One of 19 GMS users tested had access that was not required. The user, who had access to approve GMS payments, was not an employee of the Department, but worked instead for the Nebraska Children and Families Foundation; therefore, she did not need payment approval access.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, Information Security Policy 8-304 (July 2017), "Privileged Access Accounts," Section 4, states, "Privileged access accounts will have enhanced activity logging enabled."

NITC Technical Standards and Guidelines, Information Security Policy 8-502 (July 2017), "Minimum user account configuration," states the following, in relevant part:

> *(1) User accounts must be provisioned with the minimum necessary access required to perform duties*.

NITC Technical Standards and Guidelines, Information Security Policy 8-701 (July 2017), "Auditing and compliance; responsibilities; review," states the following, in relevant part:

> *An agency review to ensure compliance with this policy and applicable NIST SP 800-53 security guidelines must be conducted at least annually.*

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Access Control 6 (AC-6), Least Privilege, states, in part, the following:

> *The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.*

A good internal control plan requires procedures to ensure that user activity is tracked within the application, especially when elevated access or shared IDs are involved. Those same procedures should ensure also that each user is granted only the access necessary to perform his or her job duties, and such access is removed timely when the user terminates employment.

Without such procedures, there is an increased risk of not only inappropriate access to State assets and resources but also unauthorized processing of transactions and changes. In addition, there is an increased risk of noncompliance with NITC and NIST standards.

> We recommend the Department implement procedures to ensure that user activity can be tracked within the application, especially when elevated access or shared IDs are involved. Those same procedures should ensure also that employees are granted only the access necessary to perform their job duties, and terminated employees' access is removed timely.

Department Response: Nebraska Department of Education will develop a comprehensive internal control compliance policy to address deficiencies in user account and password management, and compliance to NITC standards. NDE plans to track suggested internal controls and audit them for implementation and effectiveness. Nebraska VR has already created a shared spreadsheet to better track user account deactivation. For CNP and GMS systems (and also to properly codify VR's practices), NDE plans to develop and implement the aforementioned compliance policy within a year.

2. <u>NITC Information Security Policy</u>

The Nebraska Information Technology Commission's (NITC) nine members are appointed by the Governor with legislative approval. Neb. Rev. Stat. § 86-516(6) (Reissue 2014) directs the NITC to do the following: "Adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel."

NITC Technical Standards and Guidelines, Information Security Policy 8-209 (July 2017), "State and agency security planning and reporting," requires or recommends State agencies to have an Information Security Plan, a System Security Plan, and a Plan of Action and Milestones Report on file. The NITC has established specific elements to be included in its Information Security Strategic Plan (8-210), System Security Plan (8-211), and Plan of Action and Milestones Report (8-212).

The APA tested the Department for compliance with some of the key elements of those NITC Technical Standard and Guidelines. Though having various documents that contained some of the necessary elements, the Department lacked documentation to support that it met all required elements, as described below.

During our review, we noted the following issues regarding the Department's compliance with the NITC Information Security Policy:

- The Department had neither a completed Information Security Strategic Plan nor a documented Data Security Control Assessment.

- The Department's System Security Plan (SSP) included a list of the systems; however, it did not include a description of the business process for each system, including a description of the function and purpose of the systems included in the SSP.

- The Department's SSP did not describe the details of where data is stored, accessed, or processed, and it did not include details of the security mechanisms applicable to this type of data.

- The Department's SSP did not describe all interfacing or connections between two or more systems or business partners.

NITC Technical Standards and Guidelines, Information Security Policy 8-209 (July 2017), "State and agency security planning and reporting," states the following:

> *The following standard and recurring reports are required to be produced by the state information security officer and each agency information security officer; these reports will reflect the current and planned state of information security at the agency:*
>
> > *(1) Information security strategic plan (section 8-210);*
> >
> > *(2) System security plan (section 8-211); and*
> >
> > *(3) Plan of action and milestones report (section 8-212).*

NITC Technical Standards and Guidelines, Information Security Policy 8-211 (July 2017), "System security plan," states the following, in relevant part:

> *Contents of the system security plan:*
>
> > * * * *
> >
> > *(6) A detailed diagram showing the flow of sensitive information, including CONFIDENTIAL and RESTRICTED information. Describe details where this data is stored, accessed, or processed and include details of the security mechanisms applicable to this type of data;*
> >
> > * * * *
> >
> > *(8) System interconnection or information sharing: Describe all interfacing or connections between two or more systems or business partners.*

NITC Technical Standards and Guidelines, Information Security Policy 8-904 (July 2017), "Data Security Control Assessment," states the following, in relevant part:

> *Each agency shall perform a security control assessment that assesses the adequacy of security controls for compliance with this policy and any applicable security frameworks (e.g., NIST, PCI, CMS, and IRS).*

Good internal control requires procedures to ensure compliance with NITC Technical Standards and Guidelines.

Without such procedures, there is an increased risk of the Department lacking formal plans that describe fully the current controls in place for protecting information at a level commensurate with the sensitivity level of the Department's systems.

A similar finding was noted during the previous audit.

> We recommend the Department implement procedures for meeting the requirements of the NITC Information Security Policy.

Department Response: Nebraska Department of Education will continue work on a System Security Plan to meet the requirements of the NITC Information Security Policy. NDE's Security and Audit committee is in process of creating the Plan which should be implemented within the next year.

3. QE2 Change Management

We tested 25 changes to the QE2 application. Six of the changes were not reviewed and approved by management and one change did not have documentation to support an appropriate segregation of duties took place from program development to migration into production. The Department's process was to have management approve the change in the tracking system utilized by the Department; however, this change was initiated and approved by the same employee.

According to the Department, a new change management process was implemented on August 12, 2019, that required changes be formally documented as well as reviewed and approved by management. Four of the six errors noted occurred prior to August 12, 2019.

NITC Technical Standards and Guidelines 8-202. Change control management (July 2017), states the following, in relevant part:

> *All IT infrastructure and application development changes are required to follow a change management process to ensure the change is approved for release and does not unknowingly add security risks to the state's environment.*

A good internal control plan requires more than one individual be involved in the development, testing, and promotion of changes to the Department's applications. When the change management procedure is not followed for all changes and changes are developed and promoted by a single employee, there is an increased risk of unauthorized, and potentially harmful, changes to applications.

> We recommend the Department strengthen its policies and procedures to ensure that the Department's change management process is followed and there is an adequate segregation of duties over changes made to QE2.

Department Response: Nebraska Department of Education will develop, within a year, a code deployment policy to help us strengthen adherence to industry standard code deployment practices.

* * * * * *

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.

Zachary Wells

Zachary Wells, CPA, CISA
Audit Manager