# 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


August 3, 2021

Matt Blomstedt, Commissioner
Nebraska Department of Education
500 S. 84th St.
Lincoln, Nebraska 68510

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, 2021 Annual Comprehensive Financial Report (ACFR) audit. This communication is based on our audit procedures through June 30, 2021. Because we have not completed our audit of the fiscal year 2021 ACFR, 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, 2021, 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 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, 2021.

## 1. User Access

The Department uses the Child Nutrition Program (CNP) to administer, including processing program claims and applications, the National School Lunch Program, Summer Food Service Program, Child and Adult Care Food Program, and the Commodity Program.

While reviewing users with access to the CNP application, the Auditor of Public Accounts (APA) noted the following:

- Three employees shared an ID that provided unrestricted access to CNP. The Department lacked procedures for formally tracking which employee had used the ID.

- Two users were listed as active in the system but had already been terminated from their employment with the State. The first terminated on May 26, 2021, and was not removed until June 25, 2021, or 21 workdays later. The second was terminated on June 1, 2021, and was not removed until June 29, 2021, or 19 workdays later. Both users were removed after the APA inquiry.

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 Information Systems and Organizations, Access Control 6 (AC-6), Least Privilege, states, in part, the following:

> *Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.*

A good internal control plan requires procedures to ensure that the individual utilizing a shared ID, with elevated access, is tracked and documented either within the application or via another tracking method. 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.

Similar findings related to CNP user access have been noted since the fiscal year 2019 ACFR audit.

> We recommend the Department implement procedures to ensure that the individual utilizing a shared ID can be adequately tracked and documented within the application or via another tracking method, especially when elevated access is 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: Over the next year the department will establish security controls from policies and procedures that will be employed to address deficiencies in identity access management in those applications that maintain standalone user directories. Security officers for these applications will be identified as part of the NDE's yearly systems inventory process and will report compliance with these controls. Remediation put in place for this finding last year by the CNP team were insufficient to address the finding, so the new centrally managed internal controls were developed and will be managed by a committee rather than individual teams.*

## 2. QE2 Change Management

The Department uses the QE2 application to track all expenses paid to assist physically or mentally disabled persons with locating jobs.

During testing of the QE2 change management process, we noted that management failed to review and approve six changes, and the explanation for that deviation from the normal approval process was not documented adequately. In addition, one of those changes lacked an appropriate segregation of duties from development to migration into production.

NITC Technical Standards and Guidelines 8-202 (July 2017), "Change control management," 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 procedures to ensure that more than one individual is involved in the development, testing, and promotion of changes to the Department's applications. Those same procedures should ensure also that any departures from the normal change management approval process are adequately explained and documented.

Without such procedures, there is an increased risk of unauthorized, and potentially harmful, changes to the Department's applications.

A similar finding was noted in the prior year.

> We recommend the implementation of procedures to ensure: 1) more than one individual is involved in the development, testing, and promotion of changes to the Department's applications; and 2) any departures from the normal change management approval process are adequately explained and documented.

*Department Response: Over the next several years, the NDE will be transitioning application development processes to Azure DevOps, a platform that will facilitate routine change management and strict auditing. Additionally, NDE has implemented an internal auditing schedule to review "anomalous" code deployments and document any such deployments. This internal auditing schedule was just implemented this year. This audit process will find and resolve any anomalous code deployments to QE2, until such time that development and deployment permissions are enforced programmatically. NDE's response to this finding in the prior year was delayed as our network team focused on keeping NDE's technology working during the pandemic.*

* * * * * *

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 suitable for any other purpose. However, this communication is a matter of public record, and its distribution is not limited.

Zachary Wells, CPA, CISA
Audit Manager