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

December 19, 2019

Matt Blomstedt, Commissioner
Nebraska Department of Education
301 Centennial Mall South
PO Box 94987
Lincoln, Nebraska 68509

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, 2019, in accordance with auditing standards generally accepted in the United States of America and the 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 19, 2019. 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 Nebraska 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 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 a 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 (Improper Payables) to be a significant deficiency.

That 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, 2019.

1. Improper Payables

The Department of Administrative Services, State Accounting Division (State Accounting), prepares the State of Nebraska 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 adequate procedures for the reporting of accurate and complete financial information to State Accounting.

The Department did not properly calculate two payables reported to State Accounting for the fiscal year ended June 30, 2019, causing an understatement of $43,335,395. The Auditor of Public Accounts proposed an adjustment for the unrecorded liabilities, and State Accounting adjusted the financial statements.

Good internal controls require procedures to ensure the accuracy of the CAFR accruals.

Without such procedures, there is an increased risk of material misstatements occurring and remaining undetected.

> We recommend the Department implement procedures to ensure the accuracy of the CAFR accruals.

Department Response: The original CAFR report submitted to DAS Accounting was correct. The understatement of $43,335,395 was a result of including two PB transactions (encumbrance/liquidation) in the reporting of actual aid expenditures for the time period July 1, 2019 through September 30, 2019 that were for the prior fiscal year. In the future NDE will make sure to only include AA ledger types when running the reports. NDE will also double check to make sure only AA ledger type payments are included. The process for running this report for completing this follow-up portion of the CAFR Report, using only Ledger Type AA, will be documented by NDE and double checked in the future.

2. CNP User Access

During testing, we noted that 12 users had inappropriate access to the Child Nutrition Program (CNP) application. The Department lacked adequate procedures for ensuring that user access was removed when no longer needed. Seven of the 12 users were USDA employees, and 5 were State employees – 4 of whom were still employed, while the other had terminated employment in April 2019.

Nebraska Information Technology Commission (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. Accounts must not be shared, and users must guard their credentials.*

A good internal control plan requires procedures to ensure that only authorized users with a business need have access to State applications.

Without such procedures, there is an increased risk for inappropriate access to State resources.

> We recommend the Department implement procedures to ensure that only authorized users with a business need have access to the CNP application.

Department Response: The Office of Nutrition Services has a current policy (updated July 2019) and procedure in place to ensure those with access to the online CNP System is applicable and necessary. The Nutrition Services' Data Analyst and Security Office have been trained to utilize the attached new user request form and policy/procedure to ensure CNP System rights are appropriately given and removed as presented. Nutrition Services will continue to monitor active State users on a quarterly basis, and inactivate any State users who no longer require access to the online CNP System.

3. GMS User Access

The Grants Management System (GMS) is a web-based system used by the Department for processing various grants and plans. During testing, we noted that one of two new users with GMS access had made no formal request or received no formal approval for such access. Additionally, during testing of 18 users with elevated access, we noted that two of those individuals had Administrator Security Group access, which allowed them to grant and remove user GMS access; however, they did not require this access as part of their job functions.

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. Accounts must not be shared, and users must guard their credentials.*

Good internal controls require procedures to ensure that documentation is on file to support a user's access to State applications. Those same procedures should also ensure that user access is restricted to what is necessary for particular job functions.

Without such procedures, there is an increased risk of unauthorized or unnecessary access to State applications.

We recommend the Department implement procedures to ensure users' GMS access is documented. We also recommend the Department periodically review access to business roles and security groups that give users elevated access, such as the ability to approve payments or the ability to give other users access.

Department Response: The Department continues to value the importance of managing user access and continues to improve the access points, integrating a single point of authentication which ensures a more rapid and efficient control of users' access to the Grants Management System at NDE. The GMS Access, Removal, and Roles policy is under revision based on APA recommendation for documented procedure implementation. The revised procedure will ensure users' GMS access/removal, and systematic review of business roles/security groups is documented and on file. Integrating these internal controls ensures a consistent application of the GMS process. The new process will be implemented by June 30, 2020.

4. NITC Information Security Policy

The Department did not have an Information Security Strategic Plan, a System Security Plan, a Plan of Action and Milestones Report, an application-specific risk assessment report, or a formal disaster recovery plan, as required by the NITC Information Security Policy.

NITC Technical Standards and Guidelines, Information Security Policy 8-206 (July 2017), "Facilities; physical security requirements," states the following, in relevant part:

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

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 8-703 (July 2017), "Security reviews; risk management," states the following, in relevant part:

> *(1) This policy is based on the NIST SP 800-53 security controls framework. Pursuant to that framework, the state must conduct an annual review of the information technology environment to ensure compliance with these standards . . . .*
>
> *The state information security officer will facilitate and oversee an annual security control assessment. This assessment will cover at least 1/3 of the control areas defined in the NIST SP 800-53 security controls, such that over a three-year timeframe all control areas will have been assessed. This review must be conducted for each major system used within the state, and must include all infrastructure and peripheral processes that are used to support state business processes.*

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) . . . . Each agency is required to have an assessment at least once every year, covering at least one-third of the applicable controls such that all control areas have been assessed over a three-year period. Agencies are also required to perform an assessment anytime significant changes to the technical environment occur.*

Good internal controls require procedures to ensure compliance with NITC Technical Standards and Guidelines.

Without such procedures, there is an increased risk of failure to identify and address threats to applications, which heightens the likelihood of a security vulnerability or threat exploitation causing such issues as downtime, loss of productivity, unauthorized access, or interference with State or Federal systems.

A similar finding was noted during the previous audit.

> We recommend the Department work with the State Information Security Officer to complete the reports required by the NITC Information Security Policy. We also recommend the Department implement procedures to ensure the periodic performance of a risk assessment that addresses specific risk associated with each application and an assessment of the criticality of each application. We also recommend the Department develop and document a formal disaster recovery plan.

Department Response: The Department continues to recognize the importance of the IT Security and determining 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 has undertaken multiple steps to expand the IT security audit procedures including the creation of a Security and Audit team to develop and implement industry standard procedures. The Security and Audit team created a risk assessment policy and are in the process of adopting a model implementation process for risk assessment of applications and the security levels associated with the efforts of a system security plan. Implementation of the assessment process and managing the ongoing support to achieve a review of the applications over a three year cycle continues. The Department has established a goal to complete an application-specific risk assessment in the 2020 fiscal year. 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. In addition, the department continues work on a formal agency-wide Continuity of Operation Plan, including the IT disaster recovery plan as part of this work.

* * * * *

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 management, 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.

Pat Reding, CPA, CFE
Assistant Deputy Auditor