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 30, 2019

Matt Blomstedt, Commissioner
Nebraska Department of Education
301 Centennial Mall South
P.O. Box 94987
Lincoln, Nebraska 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, 2018, 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 January 4, 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 (Agency) 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 Agency's management, are intended to improve internal control or result in other operating efficiencies.

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 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. Given these limitations during our audit, we did not identify any deficiencies in internal control that we consider to be material weaknesses or significant deficiencies. However, material weaknesses or significant deficiencies may exist that were not identified.

In addition, we noted other matters involving internal control and its operation that we have reported to management of the Agency, pursuant to AICPA Auditing Standards AU-C Section 265.A17, in a separate early communication letter dated September 27, 2018.

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 they will be verified in the next audit.

The following are our comments and recommendations for the year ended June 30, 2018.

1. Incorrect Information Used in Payable Calculations

During a review of changes in activity between fiscal year 2017 and fiscal year 2018, we noted one payment was not properly identified as a current-year expenditure. The payment should have been recorded as a prior-period expenditure, resulting in an understatement of expenditures and liabilities of $3,010,140. The APA's proposed adjustment was made by the Department of Administrative Services – State Accounting (DAS) to correct the error.

We noted one discretionary project payable tested was not properly calculated, resulting in an understatement of expenditures and liabilities of $97,996.

The Agency did not include the projected expenditures for Title IV in the calculation of the Grants Management System payable. This resulted in a $1,626,160 understatement of expenditures and liabilities. The Agency made the correction, and DAS made the adjustment in the financial statements.

Sound business practices and good internal controls require adequate policies and procedures to ensure expenditures are properly recorded in the accounting system, estimates for accruals are proper, and all payables are identified and properly accrued.

> We recommend the Agency establish adequate policies and procedures to record payables properly in the accounting system. We also recommend the Agency establish policies and procedures for the review of the estimates and verify all accounts and amounts are accurate and reasonable. Lastly, we recommend the Agency establish policies and procedures to ensure accruals are properly calculated prior to being submitted to DAS.

Agency Response: NDE agreed that one payment batch had been incorrectly entered and posted as a current year expenditure when it should have been coded as a previous year batch. The error had been identified by NDE after the batch had been posted, however, there is no way to make the correction in Enterprise One. DAS has been notified of the error so that the CAFR report could be adjusted.

The exclusion of the Title V grant from the CAFR was an over site by NDE. It was a new grant that all parties forgot about. It has been added and DAS has been notified.

2. CNP/GMS User Access

For 4 of 13 users tested, the users' Grants Management System (GMS) account was not deactivated timely. Access was removed 19, 32, 82, or 248 business days after termination.

Two Disability Determination Services (DDS) application developers and two DDS contract developers had full access to the production environment.

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-502 (July 2017), Minimum User Account Configuration, states, in relevant part, the following:

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

NITC Standards and Guidelines, Information Security Policy 8-303 (July 2017), Identification and Authorization, Section 4, states, in relevant part, 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, increased auditing and management supervision must be implemented.*

A good internal control plan includes a process to ensure the immediate removal of terminated users' access to GMS.

Failure to remove terminated users' access to GMS timely creates the opportunity for inappropriate access to State resources.

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.

A similar finding was noted during the previous audit.

> We recommend the Agency implement procedures to ensure that employees' access to the GMS application is removed immediately upon termination. We also recommend the Agency eliminate developer access to the database and the production environment. Alternatively, we recommend implementing compensating monitoring controls to detect changes made without management approval.

Agency Response: The department continues to value the importance of managing user access and continues to improve the access points the integrating a single point of authentication that ensures a more rapid and efficient control of user access to systems deployed at NDE.

This policy is under revision to utilize the process for decommissioning access for NDE staff and contractors utilized by the Technology Services Office. The process includes removing access to email, file servers, and other resources. Integrating the GMS and CNS access removal to this process ensures a consistent application of the process to all departing employees.

The new process will be implemented by June 30, 2019.

3. Information Technology Risk Assessment

The Agency did not have an application-specific risk assessment report or a formal disaster recovery plan completed.

NITC Standards and Guidelines, Information Security Policy 8-206 (July 2017), Facilities; Physical Security Requirements, states, in relevant part, the following:

> *Agencies must 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 8-703 (July 2017), Security Reviews; Risk Management, Section 1, states the following:

> *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 Standards and Guidelines, Information Security Policy 8-904 (July 2017), Data Security Control Assessment, states the following:

> *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). The assessment may be performed internally by the agency information security officer or with the assistance of the state information security officer. 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.*

Sound business practices and good internal controls require a risk assessment to be completed periodically and to include application-specific risk information.

Without such procedures and plans, there is an increased risk an application's threats will not be identified and planned for. This increases the risk 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 Agency implement procedures to ensure the periodic performance of an IT risk assessment that addresses specific risks associated with each application and an assessment of the criticality of each application. We also recommend the Agency develop and document a formal disaster recovery plan.

Agency Response: The Department continues to recognize the importance of the IT risk assessment. 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 cross team has created a risk assessment policy and are in the process of adopting. The department has established a goal to have at least 1/3 of applications reviewed using the process by June 30, 2019.

In addition, the department is undertaking a formal agency-wide Continuity of Operation Plan, including the disaster recovery plan as part of this work. NDE has been making progress to migrate the few remaining servers from the Nebraska State Office Building facilities into the Office of the Chief Information Officer Data Centers to take advantage of the redundancy and support.

* * * * *

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.

Philip J. Olsen, CPA, CISA
Assistant Deputy Auditor