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 23, 2018

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, 2017, 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 December 14, 2017. 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 November 27, 2017.

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, 2017.

1. DDS Rate Support

The Disability Determination Section (DDS) did not have support for 5 of 15 service rates tested. Service rates set the maximum allowed reimbursement that providers can receive for medical procedures performed. DDS did not maintain documentation to support how these reimbursement rates were determined. DDS is able to set its own rates based on what other State agencies are paying for those same types of services. DDS was reimbursing providers more than specified by either the Department of Health and Human Services (DHHS) Practitioner Fee Schedule, the Federal Medicaid Physician Fee Schedule (FMPFS), or rates approved by the Federal Administrator.

20 C.F.R. § 404.1624 (April 1, 2017) states the following:

> *The State will determine the rates of payment for purchasing medical or other services necessary to make determinations of disability. The rates may not exceed the highest rate paid by Federal or other agencies in the State for the same or similar type of service. The State will maintain documentation to support the rates of payment it uses.*

Good internal controls require support of how reimbursement rates were determined.

Good internal controls also require reimbursement rates to be reviewed periodically.

When no documentation is maintained to support how reimbursement rates were determined, and no periodic review of those rates is performed, there is an increased risk of both overpayment for services and noncompliance with Federal regulations.

> We recommend the Agency implement procedures to maintain supporting documentation of reimbursement rates and periodically review those rates.

Agency Response: Methodology used to determine the DDS vendor fee was provided to the auditors. DDSs must use a fee schedule from Federal and other State agencies to purchase similar services following SSA policy DI 39545.625. The DDS can use fee schedules from agencies other than Medicare and Medicaid. The consultative examination (CE) fee must not exceed the highest rate paid by Federal or other State agencies. The DDS fee schedule was approved by the Social Security Administration.

APA Response: As noted in the finding, there was no documentation supporting the rate paid for 5 of 15 service rates tested. For example, DDS paid up to $500 for a procedure which was last approved by the Social Security Administration in 2007, at a rate of $210. The rate, based on Current Procedural Terminology (CPT) code, per the 2017 HHS Physicians schedule was $104 and the CMS.gov physician schedule rate was $169. Our recommendation for maintaining supporting documentation for reimbursement rates is to ensure compliance with 20 C.F.R. § 404.1624. Again, that C.F.R. states, "The rates may not exceed the highest rate paid by Federal or other agencies in the State for the same or similar type of service."

2. GMS Terminated Users

For four of five users tested, the users' Grants Management System (GMS) account was not deactivated timely. Additionally, the Agency did not have procedures in place to notify the GMS vendor, MTW, when employees left the Agency in order to remove their GMS access. Additionally, for 9 of 13 users tested, GMS access forms were not on file to support that granted access was approved and appropriate.

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-101(December 2013), Section 4.7.2, User Account Management, states the following, in relevant part:

> *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 . . . .*

A good internal control plan includes a process to ensure the timely 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. When access granted to an electronic application is not documented through a formal process, moreover, there is an increased risk that unauthorized individuals could access the system, or an individual could have access that is not appropriate for his or her job function.

> We recommend the Agency implement procedures to ensure that terminated employees' access to the GMS application is removed timely. We also recommend the Agency implement procedures to document all user access to the GMS application.

Agency Response: The Nebraska Department of Education agrees with the Auditor's recommendation. The Grants Management System staff will monitor notices of staff termination sent out by the Human Resources team and end-date user accounts for terminated staff. The Grants Management System staff has also developed a new NDE System Access Request Form for this system and will have all authorized users complete an updated for to properly document their access.

3. CNP New Users

For five of five users tested, no documented approval of Child Nutrition Program (CNP) access was on file to support that granted access was approved and appropriate.

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.7.2, User Account Management, states, the following:

> *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 . . . .*

When access granted to an electronic application is not documented through a formal process, there is an increased risk that unauthorized individuals could access the system, or an individual could have access that is not appropriate for his or her job function.

> We recommend the Agency implement procedures to document user access to the CNP system, including developing a form that would indicate appropriate access for individuals and a signed-off approval by the employee's supervisor.

Agency Response: The NE Department of Education (NDE) created a policy and procedure to control access to the Child Nutrition Program (CNP) System by State employees outside of the NDE. The policy was created in May 2017 and revised in January 2018 to include the State employee's supervisor's verification of need to access the CNP system. The Data Analyst saves a PDF of the email requests for activation and deactivation of the State employees access to the CNP system.

4. Information Technology Risk Assessment

The Agency's risk assessment report lacked application-specific risk information. Additionally, the Agency did not have a formal disaster recovery plan.

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), 8-101 Section 4.5.1, Physical Security Perimeter, states, in relevant part, the following:

> *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 (December 2013), Section 4.9.3, Risk Assessment, states, in relevant part, the following:

> *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.*

NITC Standards and Guidelines, Information Technology Disaster Recovery Plan Standard 8-201 (August 2006), Section 1, Standard, states, in part, the following:

> *Each agency must have an Information Technology Disaster Recovery Plan that supports the resumption and continuity of computer systems and services in the event of a disaster. The plan will cover processes, procedures, and provide contingencies to restore operations of critical systems and services as prioritized by each agency. The Disaster Recovery Plan for Information Technology may be a subset of a comprehensive Agency Business Resumption Plan which should include catastrophic situations and long-term disruptions to agency operations.*

Good internal control requires 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 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 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.

5. DDS Developer Access

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

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.3.2.3, Separation of Duties, states 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, 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 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.

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 prior audit.

> We recommend the Agency limit access to the production environment when possible. Additionally, we recommend the Agency establish procedures to log any changes to the production environment and have someone without access to the production environment review all changes to ensure no unauthorized changes are made to the application.

Agency Response: The DDS application developers are solely responsible for development of all code and software maintenance and therefore must have access to production. For this reason, separation of duties is impractical. Compensatory controls were implemented in May of 2017. These controls include requiring supervisory approval for all changes 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 or Board, 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
Audit Manager