NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

Mike.Foley@nebraska.gov
PO Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
auditors.nebraska.gov

October 13, 2023

Jason Jackson, Director
Nebraska Department of Administrative Services
1526 K Street, Suite 190
Lincoln, NE 68508

Dear Mr. Jackson:

This letter is provided pursuant to American Institute of Certified Public Accountants (AICPA) Auditing Standards AU-C Section 265.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, 2023, Annual Comprehensive Financial Report (ACFR) and Statewide Single (Single) audits. This communication is based on our audit procedures through June 30, 2023. Because we have not completed our audits of the fiscal year 2023 ACFR or Single, additional matters may be identified and communicated in our final reports.

In planning and performing our audits of the State's financial statements as of and for the year ended June 30, 2023, in accordance with auditing standards generally accepted in the United States of America, we considered the State's system of 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.

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. However, as discussed subsequently, based on the audit procedures performed through June 30, 2023, we identified certain deficiencies in internal control that we consider to be significant deficiencies.

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.

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 Numbers 1 ("EnterpriseOne Timesheets"), and 2 ("Changes to Vendor and Banking Information") to be significant deficiencies.

We also noted certain internal control or compliance matters related to the activities of the Department of Administrative Services (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 Department, 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, 2023.

1. EnterpriseOne Timesheets

Twenty State agencies utilized EnterpriseOne (E1), the State's accounting system, to record their employees' work time entry and leave reporting. For these agencies, we noted the following:

- Supervisors and human resource staff within the State agencies were able to change the employees' submitted timesheets without the employees' knowledge or documentation of the changes made.

- E1 did not accurately track who approved timesheets in the system. For State agencies that utilized timesheet entry in E1, the supervisor assigned to an employee approved the timesheet. However, supervisors were allowed to set up delegates in the system to approve timesheets in the supervisor's absence. The system did not record who actually approved the timesheet; if a delegate approved an employee timesheet, the system would record the assigned supervisor as the approver. When delegates were set up for their supervisor, the delegate was then able to alter and approve his or her own timesheet. Furthermore, there was no audit trail for delegates in E1. When a supervisor removed a delegate from the system, there was no record of the delegates in the system in an audit trail. Supervisors were also able to delete delegates without any record of the assignment.

- Employees were able to record their time worked to other agency funding sources. When completing a timesheet, the employee had a field available to him or her to record time to any State agency. The coding was not restricted to only the employing agency.

It was also noted that Department overtime-exempt employees were not required to maintain a timesheet or other form of documentation to show that at least 40 hours were worked each week. Exempt employees were required to record only leave used in the system.

Neb. Rev. Stat. § 84-1001(1) (Reissue 2014) states the following:

> *All state officers and heads of departments and their deputies, assistants, and employees, except permanent part-time employees, temporary employees, and members of any board or commission not required to render full-time service, shall render not less than forty hours of labor each week except any week in which a paid holiday may occur.*

Sound business practices, as well as a good internal control plan, require hours actually worked by State employees to be adequately documented and such documentation to be kept on file to provide evidence of compliance with § 84-1001(1). Furthermore, a good internal control plan requires employers of employees who accrue vacation and sick leave to maintain adequate support that employees actually earned the amounts recorded in their leave records.

Section 124-86, Payroll – Agency Records, of Nebraska Records Retention and Disposition Schedule 124, General Records (February 2020), as issued by the Nebraska State Records Administrator, requires any "supporting records received or generated by an agency used to review, correct or adjust and certify agency payroll records" to be retained for five years. Per that same section, the supporting records may include timesheets and reports.

Good internal control requires procedures to ensure that the approval of timesheets is documented for subsequent review, and business units are restricted to an employee's agency. Without such procedures, there is an increased risk for fraudulent or inaccurate payment of regular hours worked or accumulation of leave. Additionally, failure to retain important payroll documentation risks noncompliance with Nebraska Records Retention and Disposition Schedule 124. When business units are not restricted, moreover, there is an increased risk that an employee may record payroll expenditures to an incorrect funding source or another agency's general ledger in error.

A similar comment has been reported since the fiscal year 2013 ACFR audit.

> We recommend the Department implement procedures to maintain adequate supporting documentation of time worked for all employees, such as timesheets or certifications, in compliance with State Statute and Nebraska Records Retention and Disposition Schedule 124. Furthermore, we recommend the Department make the necessary changes to E1, or save supporting documentation to a data warehouse, to allow for the retention of documentation of approvals, and changes to timesheets to ensure compliance with Nebraska Records Retention and Disposition Schedule 124. Lastly, we recommend the Department restrict business units to an employee's agency.

Department Response: Timesheet images are maintained in EnterpriseOne until the payroll is processed; however, the electronic data is maintained in EnterpriseOne indefinitely. Agencies choosing to delegate time approval are trained to maintain documentation when a delegate approves time. Under federal law, exempt employees do not need to track their hours. DAS – Accounting Division will work with DAS - State Personnel Division to explore ways to reconcile State and Federal law in our processes.

APA Response: Neb. Rev. Stat. § 81-1328 (Cum. Supp. 2022) outlines vacation hours earned by State employees. State employees who work less than full-time earn vacation hours in proportion to the percent of hours worked. Without a timesheet to support employee hours worked, there is an increased risk an employee will earn excess vacation leave, which is paid out upon termination.

2. Changes to Vendor and Banking Information

During our review of the process to change vendor and banking information in E1, we noted a lack of controls to ensure that additions and/or changes to vendor addresses and banking information were proper and accurate. To change vendor addresses and banking information in the system, an authorized agent at the agency level submits a W-9/ACH form to the Department. This submission can be made by a single person at the agency. There is no required secondary approval of changes at the agency level to ensure additions and changes are proper.

In addition, we noted that the Department did not perform any other procedures to identify potential fraudulent bank accounts in the system. A review could include querying for duplicate bank accounts or addresses existing for both a vendor and employee of the State.

A good internal control plan requires procedures to ensure that critical vendor and banking information within E1 is proper, and changes to the information are verified as accurate.

Without such procedures, there is an increased risk of loss, misuse, or theft of State funds due to fraudulent activity within E1.

A similar comment has been reported since the fiscal year 2015 ACFR audit.

We recommend the Department establish procedures to ensure vendor addresses and banking information in E1 are appropriate and accurate. These procedures should require a secondary approval of all vendor and banking information at the agency level when modifying W-9/ACH forms, ensuring that at least two knowledgeable individuals are involved in the changes. We also recommend the Department establish procedures, such as a periodic review for duplicate bank accounts and vendor addresses, to identify potential fraudulent bank accounts in the system.

Department Response: As a mitigating control that DAS already has in place, changes to a vendor or payee's banking information requires prior banking information be provided for verification. Changes in the past legislative session to Neb. Rev. Stat. § 81-153(10) provides a broader opportunity for vendor self-service and is being explored. DAS is working to revise its W-9 form to include agency review and approver sign-off.

3. E1 Special Handle a Voucher

The Special Handle a Voucher function (Function), a separate menu option, in the State's accounting system, EnterpriseOne (E1), allows users to change the payee of a payment voucher without going through the batch management process, which requires review by a second individual. When agencies enter payment transactions, a supplier number, which is tied to a payee number, is entered. The Special Handle a Voucher function allowed State employees to modify the payee number after the payment had been created, without requiring an approval that the change in payee was reasonable and proper. The Function was used by the following:

- The Department to provide support to agencies, so payments can continue in a timely manner if an agency lacks adequate personnel to process a transaction;
- The Department to process replacement warrants; and
- State agencies to correct vouchers without having to void and recreate another voucher.

We noted the following issues with the Function in the State's accounting system:

- Access to the Function is not restricted to only high-level users. Access was available, instead, to users who had access to Accounts Payable (AP) roles 20, 21, 30, 40, 41, 50, and 51. Essentially, anyone who had access to AP in the State's accounting system, with the exception of inquiry-only access, was able to use the Function. Due to the type of activity that can be performed with this access, we believe access should be restricted to only a limited number of high-level users. Our review noted that 811 users had access to the Function as of April 18, 2023.
- Users with the ability to add vendors and change vendor information in the State's accounting system also had access to the Function. The Address Book (AB) 50 role allowed users to add vendors and make changes to vendor information. All 11 users with AB 50 access also had access to the Function, creating an environment in which a user could set up fictitious vendors in the system or improperly change vendor information and then change payee information on vouchers to direct payment to the fictitious/modified vendor.

The Department stated that it uses the payee control-approval process within the State's accounting system, a required step in payment processing, to review and approve vendor changes made through the Function. Prior to payments being processed, transactions that have been modified using Special Handle a Voucher are sent to a queue, and then the Department must approve those transactions before a payment can be made. The Department will approve payments when the altered payee name or tax identification number is the same as the supplier; however, if the name or tax identification number do not agree, the Department will inquire with the State agency why the modification was made. This correspondence is to be maintained by the Department. While the Department has a process in place, we noted the following issues related to the payee control-approval process:

- All ten Department users with access to the payee control-approval process also had access to the Function. Thus, these users could change a payee on a voucher and then approve it, without involvement of a second person, resulting in a lack of segregation of duties.

- Two Department users with access to the payee control-approval process also had access to the Function and could add vendors or change vendor information in the State's accounting system.

While the Department was able to provide examples of transactions that were flagged by the payee control-approval process, the State's accounting system is unable to provide a population of transactions flagged for the payee control-approval process. As a result, the APA was unable to identify a population to test to ensure DAS was following their review process.

In an attempt to identify the scope of the Special Handle a Voucher use, the APA generated a possible population by running various queries in the State's accounting system. These queries identified payments where the Payee number did not agree to the Payee number tied to the Supplier number originally entered. The APA identified $11.4 million and 3,898 transactions that appeared to have required approval. The population included $7.9 million University transactions, $3.2 million State agency transactions, and $304,000 State College transactions.

From this population, the APA selected seven transactions to test to ensure that DAS had followed its review process and had documentation if the scenario required discussion with a State agency. The APA selected only seven transactions, as the original population had many instances where the Payee paid and original Supplier entered had similar names (e.g., "Iowa State University" and "Iowa State University of Science and Tech"). Of the seven transactions tested, four transactions would have been approved because the payee and supplier number all had the same tax identification number, and the other three transactions would not have required approval because they were transactions that were interfaced from the University accounting system. While the University transactions met the APA's initial criteria when generating the population, they were not modified using Special Handle a Voucher; therefore, these transactions would not have been flagged by the payee control-approval process.

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-303 (November 2022), "Identification and authorization," states, in relevant part, the following:

> *(4) 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. At a minimum, the audit of security must remain independent and segregated from the security function.*

Additionally, good internal controls require procedures to ensure an adequate segregation of duties, so no one individual is able to perpetrate and/or to conceal errors, irregularities, or fraud.

Without such procedures, there is an increased risk for errors or fraud to occur and remain undetected.

A similar comment has been reported since the fiscal year 2015 ACFR audit.

> We recommend the Department implement procedures to ensure an adequate segregation of duties. Such procedures include: 1) restricting Function access to only certain high-level users; 2) removing access to the Function for users with the ability to add vendors and make changes to vendor information in the State's accounting system; 3) maintaining documentation to support review/approval of vendor changes through the payee control approval process; and 4) preventing users with access to the payee control approval process from accessing the Function and/or adding/changing vendor information in the State's accounting system.

Department Response: Use of this process to more efficiently correct voucher issues is granted to a large user base. If the vendor/payee is changed on a voucher, a system forced process requires a DAS teammate to complete a review, and documentation from the agency is retained. This control reduces the risk for the occurrence of errors or fraud to an acceptable level. As noted in the finding, only two users had access to the payee control-approval process, Special Handle a Voucher, and vendor address book records. These users have management responsibilities over accounts payable and address book teams. DAS is reviewing the data structure around this process to evaluate options for a custom report that would allow for the identification of a population.

4. EnterpriseOne Deposit Batches

During testing of controls within the State's accounting system, EnterpriseOne (E1), we noted that users with approval access in the receipting queue were able to change a deposit after the deposit batch had been prepared by a separate user, and then approve the transaction without a secondary review and approval. This would allow the approver of the document to take monies by decreasing the deposit amount without detection by the individual who prepared the document.

Good internal control requires procedures to ensure that a proper segregation of duties exists, so no single individual is able to adjust and to approve a deposit without a secondary review by someone else.

Without such procedures, there is an increased risk of an individual perpetrating and concealing errors, irregularities, or fraud.

A similar comment has been reported since the fiscal year 2020 ACFR audit.

> We recommend the Department implement procedures to ensure no one individual is able to adjust and to approve a deposit amount without a secondary review by someone else.

Department Response: The EnterpriseOne IT team is working on a modification that would prevent an approval from making modification. For deposit batches in error, an agency would be required to delete the batch and start a new one, requiring approval.

5. PACE and CSB Application Access

The PACE (Programming Analysis Consulting Education) application is used to track the usage of the mainframe and other IT services by individual agencies and bill the agencies for the services they utilize. The CSB (Communications Services Billing) application is utilized by the Department to re-bill the cost of phone and other communication services. During our testing of users with access to the PACE and CSB applications, we noted the following:

- For 2 of the 11 users with access to the PACE application, the user's access did not appear reasonable. One of these users had terminated employment, but her access was not removed until the Department was notified by the Auditor of Public Accounts (APA), 70 days after termination. The other user was a current State contractor who did not require PACE access as part of his job function.

- For 5 of the 25 users with access to the CSB application, the user's access did not appear reasonable. Three of these users had terminated their employment with the State, but their access was not removed upon termination. These three users still had access, 91, 152, and 278 days after termination. Another user had transferred to a different agency, but his access remained 150 days after he transferred. The fifth user changed Department positions 172 days prior to the request to remove access.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, Information Security Policy 8-701 (July 2017), 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, Revision 5 (December 2020), “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.*

NITC "Technical Standards and Guidelines," § 8-502, Minimum user account configuration (July 2017), 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 and sound business practices require access to applications to be limited to necessary users only. Additionally, good internal controls require procedures to remove application access in a timely manner when the user is terminated or changes position.

When access to an application is not restricted to necessary users, or when users do not have their access removed in a timely manner upon termination or position change, then there is an increased risk of unauthorized changes being made.

> We recommend a routine review of users with access to the applications be conducted and documented, and users be removed if such access is unnecessary. We further recommend users have their access removed in a timely manner upon termination or position change.

Department Response: The OCIO agrees with the PACE & CSB access finding. A gap in the DAS teammate offboarding ticketing process was identified. The OCIO has proposed a solution within the existing offboarding process to ensure access is removed in a timely manner. Additionally, the OCIO will immediately begin to establish a documented process outlining criteria and level of access for both the PACE & CSB systems based on job function.

* * * * *

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 interim 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 purposes. However, this communication is a matter of public record, and its distribution is not limited.

Zachary Wells

Zachary Wells, CPA, CISA
Assistant Deputy Auditor