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

November 4, 2022

Lee Will, Acting Director
Nebraska Department of Administrative Services
1526 K Street, Suite 190
Lincoln, NE 68508

Dear Mr. Will:

This letter is provided pursuant to 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, 2022, Annual Comprehensive Financial Report (ACFR) and Statewide Single (Single) audits. This communication is based on our audit procedures through June 30, 2022. Because we have not completed our audits of the fiscal year 2022 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, 2022, 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.

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, 2022, we identified certain deficiencies in internal control that we consider to be significant deficiencies.

We 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 agencies and their 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.

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 (E1 Special Handle a Voucher), 2 (E1 Timesheets), and 3 (Changes to Vendor and Banking Information) to be significant deficiencies.

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, 2022.

1. E1 Special Handle a Voucher

The Special Handle a Voucher Function (Function) in EnterpriseOne (E1), the State's accounting system, allows users to change the payee of a payment voucher without going through the Batch Management Process, which requires a review by a second individual. This Function is a separate menu option within E1. The Function is 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.

- State agencies to correct vouchers without having to void and recreate another voucher.

We noted several issues with the Function in E1, including the following:

- Access to the Function is not restricted to only high-level users. As of May 20, 2022, 794 users had access to the Function, as anyone with Accounts Payable (AP) access above the "inquiry only" level were able to use the Function. Due to the ability to change the payee of a voucher with this access, we believe that such access should be restricted to only a limited number of high-level users.

- Users with the ability to add vendors and change vendor information in E1 also had access to this Function. The Address Book (AB) 50 security role allowed users to add vendors and make changes to vendor information. All 10 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 in E1, a required step in payment processing, to review and approve vendor changes made through the Function; however, we noted the following issues related to the payee control-approval process:

- All nine users with access to the payee control-approval process also had access to this 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 users with access to the payee control-approval process also had access to this Function and could add vendors or change vendor information in E1.

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-303 (March 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 control requires procedures to ensure an adequate segregation of duties, so no single 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 finding has been noted 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 E1; 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 E1.

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.

2. <u>E1 Timesheets</u>

Twenty State agencies utilized E1 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. Each employee was assigned a supervisor 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 finding has been noted 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 the 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. DAS is exploring options for capturing and retaining timesheet images each time payroll is processed.

3. 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 that 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 finding has been noted 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.

4. Clarity Program to E1 Timesheets

The Office of the Chief Information Officer (OCIO) used the Clarity program to record time worked and leave taken. Employees entered hours worked and leave used, which was then approved by their supervisor or delegate. After the timesheets were approved, the hours were uploaded to E1 for payment. From E1, the Department's Human Resources division created a payroll register and reviewed it for accuracy; however, the performance of that review was not documented. Per the Department, the undocumented review included verifying that all employees recorded 80 hours or their full-time equivalent, leave balances were positive, leave accruals and retirement were present, and holidays were paid. Due to the absence of documentation, though, the APA was unable to verify this assertion.

Additionally, the Department lacked a process for ensuring that the hours uploaded from Clarity were recorded correctly in E1. The Department performed neither a periodic reconciliation of hours from Clarity to E1 nor a periodic review to ensure that the interface between Clarity and E1 was set up correctly – both of which would help to ensure the proper recording of hours uploaded from Clarity to E1.

We tested the pay periods ending October 24, 2021, and March 27, 2022, to ensure that both the number and type of hours in Clarity agreed to those in E1. We did not note any errors. For the pay period ending October 24, 2021, 290 employees used Clarity for timekeeping, and they were paid a combined total of $786,627. For the pay period ending March 27, 2022, 280 employees used Clarity for timekeeping, and they were paid a combined total $768,479.

Good internal control requires procedures to ensure that any payroll or timesheet reviews are documented, and a periodic reconciliation or review is performed to verify that information uploaded from Clarity is recorded correctly in E1.

Without such procedures, there is an increased risk of not only failure to perform payroll or timesheet reviews, resulting in the possibility of errors going undetected, but also a lack of reconciliations between Clarity and E1, leading to mistakes that cause employees to be paid incorrectly or have their leave recorded improperly.

A similar concern has been noted since the fiscal year 2020 ACFR audit.

> We recommend the Department implement a documented review of its payroll register. We also recommend the Department perform a periodic reconciliation between Clarity and E1 to ensure that hours in Clarity are uploaded properly to E1, and all adjustments thereto are accurate.

Department Response: The Clarity team creates a Timesheet Summary Report and EnterpriseOne Report for each pay period that allows DAS Shared Services to reconcile time approved in Clarity to the EnterpriseOne upload. DAS will identify opportunities to perform a full reconciliation and document reviews performed.

5. E1 Deposit Batches

During testing of controls within 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 that 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 finding has been noted 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 continuing to review available options for restricting the approver access that allows deposit batches to be changed without a secondary review, including the possible development of an additional integrity report.

6. Workday Security Access

Workday is the State's Human Resources (HR) system. Users assigned to Workday roles or security groups are given elevated access within Workday. Roles define users with specific responsibilities and permissions when a business process runs. Security groups give users access to certain domains within Workday. In order to receive access to a Workday role or security group, a security partner at a State agency submits an email request that is approved by the Department HR Systems Coordinator. However, during our testing of users assigned Workday roles and security groups, we noted the following:

- The Department lacked a formal process for requesting and approving access to Workday security groups. It should be noted that a formal process was in place for granting access to Workday roles; however, this same process was not in place for the security groups for fiscal year 2022.

- For one of nine users tested, the user was assigned a role that was not needed to perform his job duties.

Furthermore, we noted that the Department did not perform a periodic review of elevated users' access in Workday to ensure the access was necessary to perform the users' job duties.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, Information Security Policy 8-502(1) (July 2017), "Minimum user account configuration," states the following:

> *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.*

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations (Sept. 2020), 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 the following: 1) a formal request and approval process for giving users elevated access in Workday; and 2) the performance of periodic reviews to ensure that only proper individuals are provided such elevated access.

Without such procedures, there is an increased risk of users being granted unauthorized access in Workday.

A similar finding has been noted since the fiscal year 2019 ACFR audit.

> We recommend the Department implement procedures for requesting and approving Workday security group access. Those same procedures should also provide for reviewing periodically, at least annually, such user access.

Department Response: Formal procedures for requesting and approving group access have now been put into place. When an agency needs a teammate to have new/updated access in Workday, they send a request to NIS.Security. NIS.Security forwards that request to State Personnel for review and approval or denial. A process is in place for verifying a position still needs role access when a user terminates. When someone terminates employment, the "NIS.Security team" removes the Role Assignments on that vacated position, unless the termination event is rescinded based on a request from the agency.

* * * * *

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, CPA, CISA
Assistant Deputy Auditor