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

August 12, 2021

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

Dear Mr. Jackson:

This letter is provided pursuant to AICPA Auditing Standards AU-C Section 265B.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, 2021 Annual Comprehensive Financial Report (ACFR) and Statewide Single (Single) audits. This communication is based on our audit procedures through June 30, 2021. Because we have not completed our audits of the fiscal year 2021 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, 2021, 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, 2021, 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 (EnterpriseOne 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, 2021.

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 a review by a second individual. The Function is used by the following:

- The Department to provide support to agencies, so payments can continue in a timely manner if the 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. 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 E1, 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 835 users had access to the Function as of April 21, 2021.

- Users with the ability to add vendors and change vendor information in E1 also had access to the Function. The Address Book (AB) 50 role allowed users to add vendors and make changes to vendor information. All nine 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 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 users with access to the payee control-approval process also had access to the Function and could add vendors or change vendor information in E1.

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-303 (July 2017), "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 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 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 is granted to a large user base to more efficiently correct voucher issues. 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>EnterpriseOne Timesheets</u>

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

- 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.

- E1 timesheets were maintained only for the current pay period for 18 State agencies that used the time entry function in E1.

- 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 his or her master file 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 terminated, there was no record of the delegates in the system. 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.

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 establish a policy requiring State agencies to maintain adequate supporting documentation of time worked for all employees, such as timesheets or certifications, in compliance with 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 timesheets, 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. 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/payee require prior banking information be provided for verification. DAS has prioritized the research of a vendor portal solution that can security facilitate vender self-service maintenance.

4. E1 Pay Rate Override

We noted 962 users with access to add, change, and delete information in the Speed Time Entry screen in E1, which provided users the ability to override pay rates, including their own, without approval. The Department had a procedure to identify pay rate overrides; however, the Department's procedure did not include formally documenting who performed the review, identifying what was reviewed, and documenting what action was taken. As a result, the Department lacked documentation to support a review was performed for three pay periods tested.

A good internal control plan requires procedures to ensure that no single individual has the ability to adjust his or her own pay rate, or that adequate compensating controls are in place to ensure someone does not adjust pay rates inappropriately. Those same procedures should ensure also that reviews of the Department's override reports document specifically what was reviewed, the results of those reviews, and who performed them.

Without such procedures, there is an increased risk of improper payroll adjustments being made and not identified in a timely manner.

A similar finding has been noted since the fiscal year 2017 ACFR audit.

> We recommend the Department implement procedures to ensure: 1) no single individual has the ability to adjust his or her own pay rate, or adequate compensating controls are in place to ensure someone does not adjust pay rates inappropriately; and 2) reviews of the Department's override reports document specifically what was reviewed, the results of those reviews, and who performed them.

Department Response: In January 2020, State Accounting began biweekly audits of pay rate overrides. Abnormal entries are investigated for any corrective action and addressed by the Accounting Administrator. This review procedure is now formally documented.

5. Clarity 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 HR created a payroll register and reviewed it for accuracy. However, the Department lacked a process for ensuring that the hours uploaded from Clarity were recorded correctly in E1.

We tested the pay periods ending August 30, 2020, and February 28, 2021, to ensure that the number of hours in Clarity agreed to E1 and did not note any errors. For the pay period ending August 30, 2021, 298 employees used Clarity for timekeeping, and they were paid a combined total of $802,617. For the pay period ending February 28, 2021, 292 employees used Clarity for timekeeping, and they were paid a combined total $789,496.

Good internal control requires the performance of periodic reconciliations to verify that information uploaded from Clarity is recorded correctly in E1, and any adjustments to that information are complete and accurate.

Without such reconciliations, there is an increased risk of employees being paid incorrectly or their leave not being recorded properly.

A similar finding was noted in the previous audit.

> We recommend the Department carry out periodic reconciliations to ensure that hours in Clarity are uploaded properly to E1, and all adjustments thereto are accurate.

Department Response: The Clarity team now creates a Timesheet Summary Report and NIS Report for each pay period that allows DAS Shared Services to reconcile leave approved in Clarity to the EnterpriseOne upload.

6. 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.

The lack of such procedures increases the risk of an individual perpetrating and concealing errors, irregularities, or fraud.

A similar finding was noted in the previous 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 reviewing available options for restricting the approver access that allows deposit batches to be changed without a secondary review.

7. Business Continuity Planning

The Office of the Chief Information officer (OCIO) has a Continuity of Operations Plan (COOP) which describes how the OCIO will react, respond, and recover from an incident. However, there is not a formal schedule/plan in place to conduct future tests and exercises.

Additionally, the Department has not recently completed a documented test of its process to ensure timely, continued operations of E1 at its backup site in the event the application fails at its main location. The Department's last documented test was done in March 2018. According to the Department, a partial failover test was completed in April 2020; however, no documentation was kept of this test.

Furthermore, the Information Systems Audit and Control Association (ISACA) has published the Control Objective for Information and Related Technology (COBIT) 2019 framework, which is a nationally recognized information system framework. COBIT 2019, DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP), states, in part, the following:

Test continuity on a regular basis to exercise plans against predetermined outcomes, uphold business resilience and allow innovative solutions to be developed . . . .

1. *Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP and DRP in meeting business risk.*

2. *Define and agree on stakeholder exercises that are realistic and validate continuity procedures. Include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.*

3. *Assign roles and responsibilities for performing continuity plan exercises and tests.*

4. *Schedule exercises and test activities as defined in the continuity plans.*

5. *Conduct a post-exercise debriefing and analysis to consider the achievement.*

6. *Based on the results of the review, develop recommendations for improving the current continuity plans.*

A good internal control plan and sound business practices require procedures to ensure that COOP and business continuity plans are tested periodically.

Without such procedures, there is an increased risk of prolonged interruption of government operations in the event of a disruption or failure.

A similar finding was noted in the previous audit.

> We recommend the Department implement effective business continuity controls, including periodic testing of existing recovery procedures to ensure continuity of operations of the State's accounting system in the event of disruption or failure. We also recommend the Department implement a schedule/plan of tests and exercises for its business continuity plans.

Department Response: Business Continuity and System Security Plans have been updated. An internal continuity exercise was completed in September 2020, and an additional failover exercise was successfully completed in August 2021.

8. NITC Information Security Policy

The Nebraska Information Technology Commission's (NITC) nine members are appointed by the Governor with the approval of the Legislature. Neb. Rev. Stat. § 86-516(6) (Reissue 2014) directs the NITC to do the following: "Adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel."

NITC Technical Standards and Guidelines, Information Security Policy 8-209 (July 2017), "State and agency security planning and reporting," requires or recommends State agencies to have an Information Security Plan, a System Security Plan, and a Plan of Action and Milestones Report on file. The NITC has established specific elements to be included in its Information Security Strategic Plan (8-210), System Security Plan (8-211), and Plan of Action and Milestones Report (8-212).

As a result, the APA tested some of the key elements of those NITC Technical Standards and Guidelines to verify compliance by the Department. Though having various documents that contained some of the necessary elements, the Department lacked documentation to support that it met all required elements, as described below:

- The Department had not completed an application specific risk assessment for its systems.

- Additionally, the Department's Plan of Action and Milestones Report did not include all findings from audits or other security reviews.

Good internal control requires procedures to ensure compliance with NITC Technical Standards and Guidelines.

Without such procedures, there is an increased risk of the Department lacking formal plans that describe fully the current controls in place for protection of information at a level commensurate with the sensitivity level of the Department's systems.

On July 8, 2021, the NITC significantly changed the aforementioned policies. NITC Information Security Policy 8-209 now states the following:

> *Pursuant to the terms of certain federal data exchange agreements, state agencies may be required to maintain the following documentation:*
>
> *(1) Information security strategic plan (section 8-210);*
> *(2) System security plan (section 8-211); and*
> *(3) Other information security*
>
> *For agencies not subject to federal data exchange agreements, these planning documents are considered guidelines and recommended as best practice.*

The revised policy 8-209 eliminates the prior requirement for maintenance of a Plan of Action & Milestones Report (8-212). Additionally, the NITC policy revisions have altered the contents of both the Information Security Strategic Plan and the System Security Plan. During the fiscal year ended June 30, 2021, the Department did not have any Federal data exchange agreements requiring the documentation identified in 8-209.

> While there have been significant changes to the NITC Technical Standards and Guidelines with regard to security planning and reporting, we recommend the Department review the revisions and formally document compliance with these updated requirements, specifically formally documenting a risk assessment and tracking how the Department is addressing those risks, even if not required by Federal data exchange agreements, as the NITC still recommends this as best practice.

Department Response: These policies were officially adopted by the NITC on July 8th, 2021. These updates no longer require DAS to develop an agency specific Information Security Strategic Plan (8-210), System Security Plan (8- 211), and Plan of Action and Milestones Report (8-212). DAS will review the revisions and formally document compliance with these updated requirements, specifically formally documenting a risk assessment and tracking how risks are addressed.

9. Workday User Access

Workday is the State's Human Resources (HR) system. Users assigned to Workday roles or security groups are given elevated access 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.
- For one of seven users tested, no documentation was on file to support that the State agency security partner requested the access granted.
- For two of nine users tested, documentation was not on file to support that the Department HR systems Coordinator or the Personnel Program Administrator approved the access granted.

Furthermore, we noted that the Department did not perform a periodic review of elevated users' access in Workday in order to ensure those with the elevated access needed it as part of their 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, in relevant part:

> *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 the following: 1) a formal request and approval process for giving users elevated access in applications; 2) the performance of periodic reviews to ensure that only proper individuals are provided elevated access; and 3) a formal process for requesting, approving, and reviewing user access to applications.

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

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

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

Department Response: Formal procedures for requesting and approving group access are in 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.

APA Response: The process explained by DAS was not documented in formal policies or procedures, and DAS was unable to provide documentation showing the access granted to the users tested was requested and approved."

* * * * * *

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 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
Audit Manager