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 24, 2017

Byron Diamond, Director
Department of Administrative Services
1526 K Street, Suite 240
Lincoln, Nebraska 68508

Dear Mr. Diamond:

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, 2016, 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 15, 2016. 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 Department of Administrative Services (DAS) or other operational matters that are presented below for your consideration. These comments and recommendations, which have been discussed with the appropriate members of DAS management, are intended to improve internal control or result in other operating efficiencies.

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 and, therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as discussed below, we identified certain deficiencies in the DAS 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. We did not identify any deficiencies in internal control that we consider to be material weaknesses.

A significant deficiency is a deficiency, or 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 Number 1 (CAFR Preparation) and Comment Number 2 (EnterpriseOne Business Continuity Planning – Inadequate Set up and Testing of Redundant Environment) to be significant deficiencies.

Those comments will also be reported in the State of Nebraska's Statewide Single Audit Report Schedule of Findings and Questioned Costs.

Draft copies of this letter were furnished to DAS 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 is our comments and recommendations for the year ended June 30, 2016.

1. CAFR Preparation

The Department of Administrative Services (DAS), State Accounting Division (State Accounting) prepares the State of Nebraska Comprehensive Annual Financial Report (CAFR) annually. In accordance with Neb. Rev. Stat. § 81-1125.01 (Reissue 2014), the CAFR is to be completed at least 20 days before the commencement of each regular session of the Legislature. For the fiscal year ended June 30, 2016, CAFR, this date was determined to be December 15, 2016. Therefore, the Auditor of Public Accounts (APA) agreed to a list of items to be prepared by DAS – State Accounting, with dates for submission to the APA for testing, to ensure the CAFR would be completed timely. Throughout the audit, several items were not submitted timely.

For instance, the first completed draft of the report was received on the morning of December 9, 2016, or five business days before the statutory required completion date. The APA requested that a completed first draft be submitted by November 28, 2016, in order to successfully complete our audit of the report under normal working conditions. Given the late submission of the 156-page CAFR, extraordinary effort and resources had to be utilized in order to meet the deadline.

Had any additional adjustments or issues been identified from the numerous late submissions (discussed in further detail below), or from the ongoing Statewide Single Audit, non-compliance with 81-1125.01 would have been the likely outcome. That likely outcome would have been made all the more probable by the near material Federal fund dollar amount of proposed adjustments that were not made by DAS. For this reason, we strongly suggest DAS refrain from accumulating large unadjusted amounts in future CAFR audits to mitigate the risk of a modified Independent Auditor's Report or non-compliance with State statute.

Furthermore, the draft report submitted by DAS – State Accounting was incomplete and inaccurate. DAS – State Accounting first provided an incomplete draft on December 5, 2016, in order for the APA to begin their work on the report. The incomplete draft required several revisions to correct formatting problems and incorrect information. Incomplete or missing information included disclosure for the newly implemented Governmental Accounting Standards Board Statement (GASBS) 72, Fair Value Measurement and Application, and there were continued issues with information provided for GASBS 68, Accounting and Financial Reporting for Pensions – an amendment of GASB Statement No. 27. As noted already, the final draft was not provided until December 15, 2016, which was 10 days after the date requested by the auditors and the date the report was statutorily required to be completed.

As of November 28, 2016, there were 34 past-due items that had not yet been received from DAS to complete the audit, and some information was as many as 28 days past due. The statistical information, footnotes, and management discussion and analysis ranged from 17 days to 27 days late. Some of this information was received only five business days prior to the date the CAFR was statutorily required to be completed.

During testing of the CAFR, we noted the following:

- The APA proposed 32 adjustments during the audit, 14 of which were not made by DAS – State Accounting. At the fund level, the accumulated uncorrected errors ranged from an overstatement of $8,304,385 to an understatement of $1,222,649. At the government-wide level, the accumulated uncorrected errors ranged from an overstatement of $13,513,268 to an understatement of $2,676,290. The APA also proposed adjustments, totaling $38,267,815, to correct beginning balances.

- DAS – State Accounting made several errors in the capital asset supporting documentation. Errors ranged from an understatement of $2,128,999 in buildings to an overstatement of $20,473,290 in buildings. Furthermore, DAS – State Accounting included assets as current year additions and/or deletions with dates outside of the fiscal year audited. There were also assets with dates inside of the fiscal year audited that were not included in current year additions and/or deletions.

- When making adjustments to prior period activity, State agencies record the transactions as a miscellaneous adjustment during the current fiscal year. The activity within this account should be analyzed by DAS – State Accounting, and proper adjustments should be made to ensure the financial statements are properly presented for these adjustments. DAS – State Accounting did not perform an adequate review of these accounts since only the Federal Fund was reviewed. After the APA requested DAS review all miscellaneous adjustment activity, DAS – State Accounting reviewed only line items over $1,000,000. These transactions should be reviewed at the fund level, and a lower threshold should be used when reviewing smaller funds.

- Several adjustments were necessary for missing or inaccurate State agency accrual information. For instance, the Department of Health and Human Services did not accurately report the Medicaid Drug Rebate receivable or the Third Party Liability, causing adjustments totaling $14,562,847. The Department of Economic Development understated accounts receivable by $5,490,356.

- The State Street Bank All Holdings report was used to prepare the Investment Footnote. The Holdings report initially received from DAS – State Accounting did not include two investment holdings held outside State Street Bank that totaled $3,881,529,391.

Similar findings related to errors in the preparation of the CAFR have been noted since the fiscal year 2007 audit. Adequate DAS staff resources needed to prepare and review the CAFR and supporting documentation was lacking, and these deficiencies appear to be the primary causes of the significant issues addressed in this comment, as well as similar ones preceding it for the past several years.

DAS – State Accounting did make correcting entries for all material amounts, as recommended by the APA.

A good internal control plan requires an adequate review of draft financial reports and information used to prepare the CAFR, including the information provided by other State agencies.

Without adequate procedures in place to ensure the accuracy of the financial reports and information used to prepare the CAFR, there is a greater risk material misstatements may occur and remain undetected. Furthermore, when information is not submitted to the APA on a timely basis, there is an increased risk the CAFR will not be completed timely in accordance with State statute.

> We recommend DAS dedicate or hire a sufficient number of staff to ensure internally prepared information is complete, accurate, and submitted timely to the auditors. We recommend DAS refrain from accumulating significant unadjusted amounts to help ensure the timely completion of the CAFR. We also recommend DAS continue to work with State agency personnel to ensure accrual information is supported and has a sound accounting base. Lastly, we recommend DAS – State Accounting continue to conduct periodic meetings with the APA to discuss items to be provided and issues identified during the course of the audit.

Department Response: State Accounting will continue development of procedures, training and safeguards to prevent errors in the future and to prepare, review and submit work papers and the CAFR on an accurate and timely basis.

Corrective Action Plan: State Accounting will continue to train, cross train and develop procedures internally. Additional agency level training will be developed to cover problem areas that arise during the CAFR process. State Accounting will continue the periodic meetings with APA during the CAFR process.

2. EnterpriseOne Business Continuity Planning – Inadequate Set up and Testing of Redundant Environment

DAS has hardware in place, IBM Power Systems Capacity BackUp (CBU), in case there should be a failure of EnterpriseOne (E1), the State's accounting system; however, that hardware has not been completely set up or thoroughly tested. DAS noted the CBU is set up for data replication but not as a failover system. A failover system would ensure the E1 application could

be switched over to redundant or standby equipment (and business could be continued as usual) in the event of disruption or failure of the E1 production environment. DAS indicated that, even in a best case scenario, it would take days to get the E1 application up and running using the CBU. Additionally, DAS stated the E1 application could only run off the CBU for a short time (approximately 30 days) and that other hardware would need to be set up to take over for the CBU. Accordingly, the DAS E1 business continuity planning lacks procedures that would enable a timely resumption of business processing in the event of E1 disruption or failure.

COBIT 5, a business framework for the governance and management of enterprise information technology, DSS04.02 Maintain a continuity strategy, states, in part, the following:

> *Evaluate business continuity management options and choose a cost-effective and viable continuity strategy that will ensure enterprise recovery and continuity in the face of a disaster or other major incident or disruption . . . 2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them. 3. Establish the minimum time required to recover a business process and supporting IT based on an acceptable length of business interruption and maximum tolerable outage . . . 5. Analyze continuity requirements to identify the possible strategic business and technical options . . . 8. Identify resource requirements and costs for each strategic technical option and make strategic recommendations. 9. Obtain executive business approval for selected strategic options.*

COBIT 5, DSS04.03 Develop and implement a business continuity response, states, in part, the following:

> *Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the enterprise to continue its critical activities . . . 4. Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity . . . .*

COBIT 5, DSS04.04 Exercise, test and review the BCP, states, in part, the following:

> *Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.*

Nebraska Information Technology Commission (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 procedures/hardware to be completely set up and thoroughly tested to ensure the timely resumption of business processing in the event of application disruption or failure.

When hardware intended to take over in the event of critical application failure has not been completely set up and thoroughly tested, there is increased risk of prolonged discontinuation of government processes in the event of application disruption or failure.

We recommend DAS implement effective business continuity controls, including adequate set up and testing of existing hardware or purchased hardware/services, to ensure continuity of operations for its E1 application in the event of application disruption or failure.

Department Response: DAS will establish business continuity controls to ensure continuity of operations for its JDE E1 application in the event of application disruption or failure.

Corrective Action Plan: DAS will continue developing a business continuity plan for the JDE E1 application.

3. Lease Obligations

Lease obligations were understated by $1,479,878. Terms of a building lease included a two percent increase every two years, which was not included in the DAS calculation of lease obligations. The increase was not included because DAS is attempting to renegotiate the lease agreement; however, the current agreement still contains the bi-annual increase. DAS – State Accounting declined to make an adjustment.

A similar finding was noted in the prior audit.

Sound business practices require accurate reporting of lease commitments of the State.

Without adequate processes and procedures in place to ensure the accuracy of lease obligations reported, there is an increased risk material misstatements may occur and remain undetected.

We recommend DAS implement procedures to ensure all financial information is complete and accurate.

Department Response: DAS will follow up with Building Division to ensure that all critical lease information is entered into the Pro Lease system for accurate reporting of lease commitments.

4. Capital Assets

During our review of capital assets, we noted a lack of controls to ensure additions were recorded in a timely manner and adequate documentation was maintained to support the date and cost of assets recorded in the accounting system.

We noted eight assets that were acquired in previous years but not added to the accounting system until the fiscal year ended June 30, 2016. We also noted two assets were overstated by $150,000, as credits reducing the cost of the assets were not properly recorded.

A similar finding was noted in the previous audit.

A good internal control plan and sound business practices require policies and procedures to ensure State-owned assets are recorded in the accounting system in a timely and accurate manner, so capital assets are properly reflected on the State's financial statements.

Without adequate controls in place to ensure assets are recorded timely and accurately, there is an increased risk material misstatements may occur and remain undetected.

> We recommend DAS strengthen controls by implementing policies and procedures to ensure assets are recorded timely and accurately.

Department Response: State Accounting will continue to work with agencies to ensure fixed assets are added to the State's accounting system in a timely and accurate manner.

5. EnterpriseOne Change Management

All E1 development changes are managed and logged in the E1 Object Management Workbench (OMW). This includes controlling and documenting what objects are changed, who made the change, in what environment changes are made, and the migration between the environments. A Functional Team Lead and an E1 Administrator sign off on all changes on the OMW.

The E1 team uses Clarity business management software to document E1 changes. Within Clarity, incident tickets are created and assigned to appropriate personnel who then write detailed narratives describing each change. During testing, however, we noted that four of nine changes tested were not properly documented on a Clarity ticket.

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.9.11, Change Control Management, states the following, in relevant part:

> *To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained. These change control procedures will apply to agency business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.*

Without proper and consistent change control standards, changes to systems may be made without specific approvals. This could lead to loss of data or financial data integrity, as well as unintended system downtime.

> We recommend all E1 development changes be documented in Clarity, and DAS apply consistently its change management documentation procedures to all such changes.

Department Response: DAS will document all changes in Clarity to reflect existing change management procedures and provide reinforcement training.

6. EnterpriseOne Special Handle a Voucher

The Special Handle a Voucher Function (Function) in E1, which allows users to change the payee of a payment voucher without going through the Batch Management process, is used by the following:

- DAS – State Accounting to provide support to agencies, so payments can continue in a timely manner if the agency lacks adequate personnel to process a transaction;

- DAS – State Accounting 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 is available instead to users who have access to Accounts Payable (AP) roles 20, 21, 30, 40, 41, 50, and 51. Essentially, anyone who has access to AP in E1, with the exception of inquiry-only access, is 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 813 users had access to the Function as of July 15, 2016.

- 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 allows users to add vendors and make changes to vendors. All eight 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.

DAS – State Accounting indicated 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:

- DAS – State Accounting does not maintain documentation to support its basis for approving vendor changes through the payee control approval process.

- All eight users with access to the payee control approval process also have 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 may not only access the Function but also add vendors or change vendor information in E1.

A similar finding was noted in the previous audit.

A good internal control plan requires an adequate segregation of duties to ensure that no one individual is able both to perpetrate and/or conceal errors and irregularities.

NITC Standards and Guidelines, Information Security Policy 8-101, 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 . . . .*
>
> *Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.*

When an adequate segregation of duties does not exist, there is an increased risk for errors and fraud to occur and remain undetected.

> We recommend that access to the Function be restricted to only certain high-level users. Moreover, we recommend that users with the ability to add vendors and make changes to vendor information in E1 do not have access to the Function. We recommend that documentation be maintained to support review/approval of vendor changes through the payee control approval process. Finally, we recommend users with access to the payee control approval process not also have access to the Function and/or to add/change vendor information in E1.

Department Response: DAS-State Accounting will re-evaluate the process and procedures related to Payee Control and Special Handle a Voucher functions and will make adjustments necessary to strengthen internal controls.

7. Business Continuity Planning

In our review of the Office of the Chief Information Officer (OCIO) Continuity of Operations Plan (COOP), we noted the following:

- The COOP did not include server-specific data, such as configuration files or locations, recovery file locations, dependencies between applications, etc. That information was maintained separately by each managing team. At one time, a central repository had been set up in which teams could place such pertinent business continuity information; however, it was not being utilized. This was noted in our previous audit.

- Based on discussion with OCIO staff, the COOP had not been tested for the fiscal year ended June 30, 2016.

- The COOP was last updated May 30, 2014.

A similar finding was noted in the previous audit.

COBIT 5, a business framework for the governance and management of enterprise information technology, lists the following management practices:

BAI10.01, Establish and maintain a configuration model, states the following, in part:

> *Establish and maintain a logical model of the services, assets and infrastructure and how to record configuration items (CIs) and the relationships amongst them. Include the CIs considered necessary to manage services effectively and to provide a single reliable description of the assets in a service.*

DSS04.03, Develop and implement a business continuity response, states the following, in part:

> *Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the enterprise to continue its critical activities . . .*
>
> *4. Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity . . .*

DSS04.04, Exercise, test and review the BCP, notes the following:

> *Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.*

NITC Standards and Guidelines, Information Technology Disaster Recovery Plan Standard 8-201 (August 2006), Section 1, states, "The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency." This section notes, among others areas, that the plan must include an "[a]nnual plan review, revision, and approval process."

A good business continuity plan, which encompasses disaster recovery planning, includes making available reliable and useful information for decision making when faced with a disaster or other event causing or creating the potential for a loss of business continuity. A good business continuity plan also includes regular testing and updating of the plan.

When reliable and useful information is not available for business continuity purposes, and when the COOP is not tested and updated, there is an increased risk of extended downtime of vital State services.

> We recommend the OCIO work to continue improving business continuity and disaster recovery plans to include a central, backed-up repository of all reliable and useful information for resuming State information technology resources and to test and update the COOP annually.

Department Response: DAS-OCIO has completed work to review, update and prioritize mission essential functions for the continuity plan during 2016. The updated plan includes detailed information of resources, actions and procedures to ensure the execution of the OCIO mission essential functions in the event of an emergency and/or immerging threat that incapacitates normal business activities at the primary operating facility.

8. Workday User Access Review and Users with Access to Change Pay

Workday is human resource business process software utilized by the State. The Workday Service Organization Control type 1 (SOC1) report for the period ended April 30, 2016, lists various complimentary customer controls that Workday customers are expected to implement. One such control warns, "Customers are responsible for controlling the access rights and authorization limits necessary for each end user to accomplish job responsibilities."

However, DAS did not complete a periodic documented review of users with access to Workday. Within Workday, users can be assigned to various roles or security groups. Assignment to these roles or groups allows the users to perform various tasks. For instance, HR Partners and HR Administrators are able to change compensation information, and Benefits Administrators are able to set up benefits and initiate and approve employee benefit events.

DAS indicated that it currently performs security access and authorization limit reviews on an informal basis but is yet to develop, conduct, and document a more formalized process. As a result of not performing such a review, DAS was not aware that eight State Personnel Office employees had access to initiate compensation changes. DAS agreed these employees did not need this access – and, following the APA's inquiry, removed the access.

NITC Standards and Guidelines, Information Security Policy 8-101, 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 . . . .*
>
> *Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.*

When user access to applications is not periodically reviewed, it creates the opportunity for inappropriate access to State resources. When users are assigned access they do not require to complete their job functions, it creates the opportunity for inappropriate system changes.

> We recommend DAS implement procedures to complete a periodic, documented review of users with access to Workday. This review should include all Workday users assigned to Workday roles and Workday security groups, especially users with access to change compensation information in Workday.

Department Response: DAS will complete the review of Workday Security Groups and User Roles; who is in them, how they are assigned, and the approval process.

9. EnterpriseOne Terminated User Access

For 24 of 25 terminated users tested, access to E1 was not disabled or removed in a timely manner (within three business days). Two of these users accessed the system after their termination date. The delay in disabling the user ID's ranged from 4 to 98 business days.

A similar finding was noted in the previous audit.

NITC Standards and Guidelines, Information Security Policy 8-101, 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 . . . .*
>
> *Agencies or data owner(s) should perform annual user reviews of access and appropriate privilege.*

Nebraska State Accounting Manual, AM-005, General Policies, Section 32, Terminated Employee Payroll and Financial Center ID's, states the following, in relevant part:

> *Each agency shall have a documented procedure to immediately disable the ENTERPRISEONE ID of an employee who has terminated employment with the agency. It is the responsibility of the agency's authorized agent to request termination of the User ID from the computer system within five working days from the termination date . . . .*

A good internal control plan includes a process to ensure the timely removal of terminated users' access to E1.

When terminated users' access to E1 is not removed timely, it creates the opportunity for inappropriate access to State resources, as well as unauthorized processing of transactions.

> We recommend DAS work with State agencies, through on-going training and monitoring of agency personnel, to ensure agencies request termination of E1 user ID's prior to, or immediately upon, termination. We recommend agencies trigger such requests by entering employee termination dates in Workday as soon as a termination date is determined, which may be prior to the termination date.

Department Response: DAS will continue training of agency HR partners regarding agency responsibilities to deactivate a terminated user's access on a timely basis.

10. E1 Timesheets

Seventeen State agencies utilized E1 to record their employees' work time entry and leave reporting. For these 17 agencies, we noted the following:

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

- For 3 of 25 employees tested, timesheet approval was not properly documented.

- E1 timesheets were maintained only for the current pay period for 15 State agencies that used the time entry function in E1.

- Supervisors and human resource staff within the State agencies were able to change the employee's submitted E1 timesheet without the employee's 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.

A similar finding was noted during our prior audits.

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 also 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, 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.

A good internal control plan requires the approval of timesheets to be documented for subsequent review.

Without adequate records to support hours worked and approvals in the E1 system, there is an increased risk for fraudulent or inaccurate payment of regular hours worked or accumulation of leave. Additionally, failure to retain important documentation risks noncompliance with Nebraska Records Retention and Disposition Schedule 124.

> We recommend DAS – State Accounting establish a policy requiring all employees of State agencies to maintain adequate supporting documentation, such as timesheets or certifications, in compliance with the Nebraska Records Retention and Disposition Schedule. Furthermore, we recommend DAS – State Accounting 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 the Nebraska Records Retention and Disposition Schedule.

Department Response: Time sheet images are maintained in the system of record (E1) until the payroll is processed; however, the electronic data is maintained in E1 indefinitely. Agencies will be reminded to retain any information they may receive, generate or create outside of the E1 system in support of an agency's payroll to be done in accordance with Nebraska Records Retention and Disposition Schedule 124.

11. 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 additions and/or changes to vendor addresses and banking information are proper and accurate. To change vendor addresses and banking information in the system, an authorized agent at the agency level submits a form W-9/ACH to DAS – State Accounting. 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 DAS – State Accounting does not perform any other procedures to identify fraudulent bank accounts in the system, such as a review for duplicate bank accounts and vendor addresses for the same vendor, since employees can also be vendors for the State.

A similar finding was noted in the previous audit.

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

A lack of adequate policies and procedures for the review and approval of vendor and banking information in E1, as well as any changes thereto, increases the risk of loss or misuse of State funds due to fraudulent activity.

> We recommend DAS establish policies and procedures to ensure vendor addresses and banking information is appropriate and accurate. These policies and procedures should include modifying form W-9/ACH to require a secondary approval of all vendor and banking information at the agency level to ensure two knowledgeable individuals are involved in changes. We also recommend DAS establish policies and procedures to identify fraudulent bank accounts in the system, such as a periodic review for duplicate bank accounts and vendor addresses.

Department Response: DAS will continue reviewing Address Book policies and procedures including a review of procedures to identify duplicate bank accounts and vendor addresses.

12. EnterpriseOne AS/400 Access Log Review

In our examination of the DAS – State Accounting review process over access logs of the AS/400 computer, where the E1 application resides, we noted the following:

- A daily system log for users that accessed the AS/400 is normally generated automatically, saved on a shared drive, and reviewed monthly. DAS – State Accounting did not document its review of the daily system logs of users accessing the AS/400 during the audit period.

- A DAS – State Accounting employee who has access to the E1 AS/400 system accounts also performs a review of system account access logs. System accounts are ID's used for upgrades and are shared by the E1 team for system maintenance. The daily system logs show logins but not which team member used the ID's to access the AS/400. According to a DAS – State Accounting staff member, team members are instructed to log their use of AS/400 system ID's in SharePoint. SharePoint is a web application in the Microsoft Office suite that can be used to store, track, and manage electronic documents. A DAS – State Accounting supervisor compares the AS/400 login report to SharePoint to determine if systems ID's are being used properly. However, this same employee also has access to the system accounts. To ensure a proper segregation of duties, this review should be performed by someone without such access. In addition, our review noted the DAS – State Accounting IT supervisor did not document her review of these system account logs. Our review also noted that DAS – State Accounting team members did not log every use of the system accounts, causing the log in SharePoint to be inconsistent with actual use.

A similar finding was noted in the previous audit.

Sound business practice and a good internal control plan require procedures to generate and review daily system logs for highly sensitive access. Sound business practice and a good internal control plan also require a segregation of duties to ensure the individual reviewing special account access does not also have access to the special accounts.

When system user account logs are not generated or reviewed, a review is not documented, and there is a lack of segregation of duties, there is increased risk of improper system access.

> We recommend DAS develop a procedure to document its review of AS/400 daily system logs. We recommend that use of AS/400 system accounts be consistently documented. We further recommend that review of system account use logs be assigned to someone who does not have access to system accounts. This review should be documented.

Department Response: DAS will review procedures to document reviews of AS/400 daily system logs.

13. EnterpriseOne AS/400 Users

DAS did not perform an annual review of users with access to the AS/400 computer system, where the E1 application resides. During our review of users with AS/400 access, we inquired of DAS IT staff regarding their process for reviewing such access. The APA was informed that no such review had been completed during the audit period.

NITC Standards and Guidelines, Information Security Policy 8-101, 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 . . . .*
>
> *Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.*

Lack of a documented review of AS/400 access allowed two consultant users to maintain access to the computer system past the date that they required such access.

> We recommend DAS implement procedures to review periodically, at a minimum annually, user access to its applications.

Department Response: DAS will establish a procedure to annually review user access to the AS/400.

14. Human Resource User Role 65

We noted several payroll batches involving DAS payroll that were prepared, approved, and posted by a single DAS payroll employee.

A good internal control plan includes an adequate segregation of duties to ensure at least two individuals are involved in processing payroll payments.

The Human Resource User Role 65 (HR 65) in E1 was used by DAS – State Accounting to perform the final update processing for payroll. However, the HR 65 role also allows users to prepare, approve, and post transactions, as this role is not set up with batch management. We noted several payroll journal entries and vendor payroll deduction batches, including batches that contained DAS payroll that were prepared, approved, and posted by a single DAS employee.

A similar finding was noted in the previous audit.

> We recommend DAS ensures any batches involving its own payroll be processed by at least two separate individuals.

Department Response: DAS will review procedures for processing internal payrolls.

* * * * *

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 DAS 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 DAS.

This communication is intended solely for the information and use of DAS, the Governor and State Legislature, others within DAS, 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