



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 31, 2017

Corey Steel, Court Administrator
Nebraska Supreme Court
State Capitol, Room 1213
Lincoln, Nebraska 68509

Dear Mr. Steel:

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 Nebraska Supreme Court (Supreme Court) or other operational matters that are presented below for your consideration. These comments and recommendations, which have been discussed with the appropriate members of the Supreme Court's 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. Given these limitations during our audit, we did not identify any deficiencies in the Supreme Court's internal control that we consider to be material weaknesses or significant deficiencies. However, material weaknesses or significant deficiencies may exist that were not identified.

Draft copies of this letter were furnished to the Supreme Court to provide management with an opportunity to review and to respond to the comments and recommendations contained herein. All formal responses received have been incorporated into this letter. Responses have been objectively evaluated and recognized, as appropriate, in the letter. Responses that indicate corrective action has been taken were not verified at this time, but they will be verified in the next audit.

The following are our comments and recommendations for the year ended June 30, 2016.

1. Accounts Payable Accrual

The Department of Administrative Services, State Accounting Division (State Accounting), prepares the State of Nebraska Comprehensive Annual Financial Report (CAFR) and requires all State agencies to determine and report payable and receivable amounts at the end of the fiscal year on an accrual response form.

The Supreme Court's Fee for Service system cannot identify transactions as prior period obligations when it interfaces with the State's accounting system. Consequently, a manual adjustment is necessary to record the accounts payable amount for CAFR reporting purposes.

The Auditor of Public Accounts (APA) noted several issues with the accounts payable amount reported to State Accounting for inclusion in the CAFR, including the following:

- The accounts payable amount of \$5,071,179 originally submitted to State Accounting did not separate out amounts payable from cash funds and amounts payable from general funds. The amount that should have been recorded to cash funds was \$270,249. The Supreme Court corrected the error after being brought to its attention by the APA.
- The original report used to calculate the accounts payable amount was generated incorrectly. Using the correct report resulted in the accounts payable amount decreasing by \$5,440. No adjustment was proposed or made for this amount.
- A similar accounts payable accrual was not calculated for fiscal year 2015. Consequently, a beginning balance adjustment would be necessary. However, the Supreme Court did not calculate a beginning balance adjustment. The APA-calculated adjustment was \$5,445,312 for general funds and \$490,540 for cash funds. State Accounting passed on the APA's proposed adjustment.
- The Supreme Court reviewed only claims with a general ledger date from July 1, 2016, through August 9, 2016, in the State's accounting system when calculating the accounts payable amount. It appears reviewing claims through August 31st would be more reasonable and result in a more accurate accounts payable amount. The APA reviewed claims from August 10th through August 31st and noted an additional \$395,588 that should have been included in the accounts payable amount. No adjustment was proposed or made for this amount.
- During a detail testing of claims, the APA noted three of three claims tested were not included in the accounts payable amount. However the claims were actually for services provided prior to June 30, 2016, and, therefore, should have been included in the accounts payable amount. These three claims totaled \$4,928. No adjustment was proposed or made for this amount.

A good internal control plan requires agencies to have adequate procedures for the reporting of accurate and complete financial information to State Accounting for inclusion in the CAFR.

When accounts payable amounts are not reported accurately, there is an increased risk the State's financial statements will be materially misstated, and those misstatements will remain undetected.

We recommend the Supreme Court implement procedures to accurately identify the accounts payable amount at fiscal year end. Such procedures should include a documented review by appropriate management.

Supreme Court Response: The Supreme Court will review current procedures and implement new processes with the goal of improving the accuracy of fiscal year end accounts payable amounts.

2. JUSTICE Change Management Procedures

In our review of the change management process of the Judicial User System to Improve Court Efficiency (JUSTICE) application, we noted that the change management documentation system, Bug Tracker, utilized by the Supreme Court was not directly tied to actual changes placed into production within Implementer, a tool used to track and implement changes to JUSTICE by the Office of the Chief Information Officer (OCIO).

In our review of the change management process for the JUSTICE application, we obtained a listing of actual changes made to the JUSTICE production environment during the fiscal year ended June 30, 2016, from Implementer. We selected 25 Implementer change requests, and we tested all 55 changes reflected on these 25 Implementer change requests. For 14 of 55 changes, we were unable to trace the actual change made in Implementer to the Supreme Court's change management documentation system, Bug Tracker, as no service requests were generated for these changes. Although the Supreme Court indicated it periodically obtains and reviews reports from Implementer showing JUSTICE changes to ensure changes are appropriate and authorized, this review process does not appear adequate given the significant number of changes we tested that were not supported by a service request.

We also noted that 10 user IDs, 6 contracted programmers, and 4 OCIO employees had move and checkout access to the JUSTICE development, test, and production environments. Three of the four OCIO employees also had access to push changes out to the county AS/400s using the System AS/400.

A similar finding was noted during the previous audit.

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.

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.3.2.3, Separation of Duties, states the following, in relevant part:

To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical. Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, audit trails and management supervision must be implemented.

A good internal control plan includes a formal methodology to guide the development of applications and systems. Changes to existing applications and systems should undergo initial evaluation, authorization, and implementation procedures to ensure they have met expectations and minimized user disruption. These processes should be adequately documented.

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

We recommend the Implementer software used to make the actual changes to the JUSTICE application note or in some way relate to the change management documentation within Bug Tracker. Additionally, we recommend the Supreme Court's review of Implementer changes include verification that all changes have a corresponding service request. Also, we recommend the Supreme Court implement an adequate segregation of duties to prevent users from checking out code, developing, and promoting changes without secondary review and approval.

Supreme Court Response: The Supreme Court has begun reviewing Implementer reports to verify that there is a corresponding service request. Documentation is kept of the reviews. The Supreme Court does not manage the access of OCIO employees. The Supreme Court has no objections to the OCIO removing the file move and checkout access from their employee's user accounts.

3. Annual Review of JUSTICE IDs

There was no documented review of JUSTICE user IDs during the fiscal year ended June 30, 2016. The last review was performed on June 23, 2015.

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.

We recommend the Supreme Court implement procedures to periodically review, at a minimum annually, user access to its applications.

Supreme Court Response: The Supreme Court will work with the OCIO to ensure annual reviews of JUSTICE IDs are completed.

4. JUSTICE New Users

For 2 of 23 users tested, the access provided did not appear reasonable, as the actual access granted did not match access explicitly expressed on access request forms.

The Supreme Court indicated that, after receiving an Access Request Form, it follows-up with a phone conversation to verify the access the user needs, but the Supreme Court did not maintain documentation to support changes made to access based on such conversations.

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, provides 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

When users have access to applications that are unnecessary or unreasonable for the performance of their job duties, it creates the opportunity for inappropriate access to State resources, as well as unauthorized processing of transactions.

We recommend the Supreme Court document the appropriate access for all users. This could be accomplished by completing a new Access Request Form or documenting communication between the users/supervisors and Supreme Court Staff on the Access Request Form.

Supreme Court Response: The user request form is being amended to better reflect current access options. In addition, documentation will be kept of any changes to user access after initial access has been granted.

5. JUSTICE Security Settings

The JUSTICE application is used by the county and district courts to record all financial and case activity. The JUSTICE application resides on both a Supreme Court AS/400 computer and on county AS/400s. Users of the JUSTICE application residing on the Supreme Court AS/400, including Supreme Court employees, must re-authenticate after four hours of inactivity. Users of

the JUSTICE application residing on the county AS/400s, including county employees and various Supreme Court employees, are never required to re-authenticate (outside of the hours of 6:00 PM to 7:00 PM, when the timeout setting is set at 30 minutes). While the NITC Standard 8-101 does not indicate what the “predetermined period of inactivity” should be, four hours does not appear reasonable and in-line with the intent of the standard to prevent unauthorized access to information.

A similar finding was noted during the previous audit.

Nebraska Information Technology Commission (NITC) Standards & Guidelines (December 2013), Information Security Policy 8-101, Section 4.5.4, Clear Screen, states the following:

To prevent unauthorized access to information, agencies will implement automated techniques or controls to require authentication or re-authentication after a predetermined period of inactivity for desk tops, laptops, PDA's and any other computer systems where authentication is required. These controls may include such techniques as password protected screen savers, automated logoff processes, or reauthentication after a set time out period.

A good internal control plan includes utilizing re-authentication rules that require users to comply with the NITC standards.

An excessive period of inactivity between required re-authentication increases the risk of an unauthorized user gaining access to confidential information and key financial data.

A similar finding was noted during the previous three engagements. Our prior audit recommended that the Supreme Court set its re-authentication setting to a more reasonable level, such as 30 minutes or less. The Supreme Court responded to this prior year recommendation as follows:

The Administrative Office of the Courts will discuss this issue with the OCIO's Intergovernmental Data Services Division, the DMV, and a NACO representative for the counties which will be affected to determine if a 30 minute re-authentication setting can be implemented.

We recommend the Supreme Court work with the Department of Motor Vehicles and the OCIO to implement a re-authentication setting for the AS/400s. We recommend a timeout setting of 30 minutes or less.

Supreme Court Response: JUSTICE re-authorization settings are determined by the OCIO, not the Supreme Court. The Supreme Court, in 2016, did request that the OCIO change settings, but no action was taken. The Supreme Court will document further attempts to work with the OCIO and the Department of Motor Vehicles.

6. JUSTICE User Termination

The Supreme Court did not have an adequate process to ensure JUSTICE user access was removed in a timely manner upon user termination. We noted 14 JUSTICE users still had access to JUSTICE after their termination dates. Four of these users signed on to the JUSTICE AS/400 after termination.

A similar finding was noted during the previous audit.

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.

A good internal control plan includes a process to ensure terminated users' access in JUSTICE is removed timely.

When access to applications is not terminated timely, it creates the opportunity for inappropriate access to State resources.

We recommend the Supreme Court implement procedures to ensure user access to JUSTICE is removed upon a user's termination.

Supreme Court Response: The Supreme Court will continue to improve processes regarding terminating user access. Note that many JUSTICE users are county employees. Notice, by counties, of employee termination is not always received by JUSTICE on a timely basis.

7. Bank Accounts Not Under Control of the State Treasurer

The APA identified bank accounts that were opened and operated under the State's Federal Tax Identification Number (FTIN) without the express prior authorization of the State Treasurer. In these specific instances, the Supreme Court appears to have the authority to administer the separate County Court accounts or funds under the State's FTIN. When establishing the banking relationship necessary to exercise that authority, however, the State Treasurer's approval must be obtained.

According to State law, one of the duties of the State Treasurer is to establish banking relationships for the State of Nebraska. Below is a summary of the bank accounts identified by the APA as being maintained without the State Treasurer's approval, as of June 30, 2016.

a) Nebraska County Court Accounts

During the fiscal year 2015 CAFR audit, the APA found that the County Courts in Nebraska maintained over 120 different bank or investment accounts with a combined balance of over \$11 million at June 30, 2015. As of June 30, 2016, these accounts were still not established through the State Treasurer but rather by each County Court, under the supervision of the Nebraska Supreme Court offices.

Neb. Rev. Stat. § 25-2713 (Reissue 2016) allows for the investment of County Court funds, as provided by the rules of the Supreme Court. Neb. Rev. Stat. § 24-511 (Reissue 2016) gives the clerk certain powers, including receiving and depositing money received by the County Court. Additionally, § 6-1450(A)(1) of the Supreme Court Rules directs such funds to be deposited into bank accounts designated by the county judges.

As the above-referenced statutes and rule make clear, the County Courts are empowered to utilize, under the administrative supervision of the Supreme Court, certain statutorily created funds. Doing so necessarily entails opening bank accounts – and, because of the Supreme Court’s supervisory role, those accounts utilize the State’s FTIN. Nevertheless, as pointed out previously herein, the Attorney General has stated in Op. Att’y Gen. No 15-010 (Aug. 10, 2015), “A state agency is not permitted to contract for its own banking relationship.” This is because, that opinion declares, “The State Treasurer is charged with the duty of establishing the banking relationship for the State of Nebraska and its agencies.” Previously, in Op. Att’y Gen. No 98006 (Jan. 22, 1998), the Attorney General had stated, “We are unaware, generally, of any other statutes which specifically give other state officials or state agencies the authority to deposit the state’s funds in a bank.”

Thus, maintaining County Court bank accounts under the State’s FTIN without the proper authorization intrudes upon the sole authority of the State Treasurer to establish banking relationships that utilize that unique identification number. Additionally, allowing accounts to be opened and operated under the State’s FTIN without the approval of the State Treasurer may result, moreover, in loss or misuse of public funds or give rise to concerns regarding insufficient pledged collateral to secure the amount of money in excess of FDIC coverage.

We recommend the Supreme Court work with the State Treasurer to ensure the proper authorization is obtained prior to opening any County Court bank accounts utilizing the State’s FTIN. The State Treasurer’s approval should be documented and maintained on file.

Supreme Court Response: The Supreme Court is in the process of developing an agreement with the State Treasurer regarding approval of bank accounts that use the State FTIN. Those bank accounts that relate to specific court cases and do not contain State funds will continue to be under the oversight of the Supreme Court.

8. State Bank Account Not Utilizing State’s FTIN

The APA identified one County Court bank account that was still not recorded under the State’s FTIN at June 30, 2016. This bank account, ending in 917, was opened by the Grant County Court, which operates under the administrative supervision of the Nebraska Supreme Court.

Because County Court offices fall under the Supreme Court and not under the particular County function, any bank accounts opened by them should bear the State’s FTIN. Therefore, like all other County Court bank accounts, the account maintained by the Grant County Court should also be utilizing the State’s FTIN.

A good internal control plan requires procedures to ensure that bank accounts held by County Courts, which are subject to the administrative supervision of the Supreme Court, are correctly identified under the State's FTIN.

When County Court bank accounts are recorded under the incorrect FTIN, there is an increase risk for the loss or misuse of public funds.

We recommend the Supreme Court Administrator's office work with the Grant County Court and the State Treasurer to ensure the bank account at issue is utilizing the State's FTIN, as authorized by the State Treasurer. The State Treasurer's approval should be documented and maintained on file.

Supreme Court Response: This finding has been resolved. The bank account for Grant County Court now uses the State FTIN as of December 31, 2016.

* * * * *

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 Supreme Court 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 Supreme Court.

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