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

December 19, 2019

Corey R. Steel, State Court Administrator
Nebraska Supreme Court
Nebraska State Capitol, Suite 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, 2019, in accordance with auditing standards generally accepted in the United States of America and the 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 19, 2019. 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 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.

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 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.

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 internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been 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, 2019.

1. Unauthorized Bank Accounts

During the fiscal year ended June 30, 2015, the Auditor of Public Accounts (APA) performed a statewide review of bank accounts using the State's Federal Tax Identification Number (FTIN) without the documented approval of the Nebraska State Treasurer. The APA performed follow-up procedures and noted that only one such account still existed during the fiscal year ended June 30, 2019. The bank account was for a court case that had yet to be settled. The account balance at June 30, 2019, was $40,962. Furthermore, the Supreme Court established an additional account under the State's FTIN, with a balance of $219,017 at June 30, 2019. This account also lacked documented approval from the Nebraska State Treasurer to use the State's FTIN.

Neb. Rev. Stat. § 77-2301(1) (Reissue 2018), provides, as is pertinent, the following:

> *The State Treasurer shall deposit, and at all times keep on deposit for safekeeping, in the state or national banks, or some of them doing business in this state and of approved standing and responsibility, the amount of money in his or her hands belonging to the several current funds in the state treasury.*

Likewise, Neb. Rev. Stat. § 77-2309 (Reissue 2018) says the following:

> *It is made the duty of the State Treasurer to use all reasonable and proper means to secure to the state the best terms for the depositing of the money belonging to the state, consistent with the safekeeping and prompt payment of the funds of the state when demanded.*

In Op. Att'y Gen. No 15-010 (Aug. 10, 2015), the Nebraska Attorney General stated the following:

> *A state agency is not permitted to contract for its own banking relationship; all such relationships are established through the State Treasurer.*

Neb. Rev. Stat. § 24-215 (Reissue 2016) states, in relevant part, the following:

> *The Clerk of the Supreme Court shall, on the first day in January, April, July, and October of each year, pay into the General Fund of the state treasury all fees of every nature and description received by him or her during the preceding three months; and the State Treasurer shall issue his or her receipt for such fees.*

Good internal controls require procedures to ensure that the State's FTIN is not used without the express authorization of the State Treasurer.

Without such procedures, there is an increased risk of not only loss or misuse of State funds but also improper intrusion upon the statutory and inherent constitutional authority of the State Treasurer to oversee the State's banking relationships.

> We recommend the Supreme Court obtain the formal approval of the State Treasurer before utilizing the State's FTIN.

Supreme Court Response: The Supreme Court is currently renewing the agreement with the State Treasurer regarding accounts used by the courts on a daily basis. In addition, the Supreme Court is working with the Treasurer's office to develop a process for notifying their office of bank accounts associated with a specific court case.

2. JUSTICE Terminated User Access

The JUSTICE application is the Supreme Court's case and financial management system for Nebraska trial courts. Employees of various State agencies, including the Supreme Court, and counties and cities across Nebraska had access to the application during the fiscal year. During testing of terminated employees of those State and local entities, it was noted that 11 terminated State users, 13 terminated county users, and four terminated city users did not have their access removed in a timely manner, within three business days of termination.

When a user with JUSTICE access is terminated, it is the responsibility of the employee's management to notify the JUSTICE team immediately of the termination, so the former employee's access can be removed without delay. Of the 28 terminated employees tested, the JUSTICE team was notified of only seven terminations; of those seven, one did not have her access removed within three days of termination. Instead, her access was removed 88 days after the employee had terminated and 99 days after the JUSTICE team was notified.

During testing, it was noted also that two State and two county users had "Previous Sign On" dates that followed their respective termination dates – meaning it appeared that they had been able to access the JUSTICE application after the conclusion of their employment.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, Information Security Policy 8-701 (July 2017), "Auditing and compliance; responsibilities; review," states the following, in relevant part:

> *An agency review to ensure compliance with this policy and applicable NIST SP 800-53 security guidelines must be conducted at least annually.*

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Access Control 6, "Least Privilege," states, in part, the following:

> *The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.*

Good internal controls require procedures to ensure that access to the JUSTICE application is disabled timely upon termination of the user's employment.

Without such procedures, there is an increased risk of a former employee continuing to access the JUSTICE application improperly.

We recommend the Supreme Court implement procedures to ensure access to the JUSTICE application is disabled timely upon termination of the user's employment. Additionally, we recommend the Supreme Court inform counties and city departments of the responsibility to notify immediately the JUSTICE team upon termination of an employee with access to the application.

Supreme Court Response: For judicial branch staff, the Supreme Court will examine the employee exit process and determine where improvements could be made to ensure terminated users' access to JUSTICE is removed in a timely manner.

In order to access JUSTICE, external entities must currently sign a user agreement. That agreement contains an obligation for those entities to notify the Supreme Court of termination of any employee. Subsequent to the audit, the Supreme Court IT Division has contacted several county offices to remind them that JUSTICE accounts are non-transferable between employees.

The Supreme Court also contends that the risk of improper access is reduced since any individual, once separated from state or county employment, would no longer have access to a computer that is on the state network, or that is authorized to access the state network. JUSTICE is not accessible from outside of the state firewall, therefore, any JUSTICE account information still held by the individual would be unusable.

3. NITC Information Security Policy

The Nebraska Information Technology Commission (NITC) is a nine-member commission, whose 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."

Per the NITC's "Technical Standards and Guidelines," § 8-209, *State and agency security planning and reporting* (July 2017), State agencies must have an Information Security Strategic 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). The APA tested some of those key elements to verify compliance by the Supreme Court. Though having various documents that contained some of the necessary elements, the Supreme Court lacked documentation to support it met all required elements.

Good internal controls require procedures to ensure that all elements of the Information Security Strategic Plan, System Security Plan, and Plan of Action and Milestones Report are on file, as required by the NITC Information Security Policy.

Without such procedures, the Supreme Court lacks formal plans that fully describe the current controls in place for protecting information at a level commensurate with the sensitivity level of the Supreme Court's systems.

We recommend the Supreme Court work with the State Information Security Officer to complete the reports required by the NITC Information Security Policy.

Supreme Court Response: The Supreme Court has a designated Security Officer and maintains a library of security documentation, which is reviewed and updated as a part of the IT Division's continuous process for security enhancement. These documents contain the elements of what is described in NITC standards 8-210, 8-211, and 8-212.

All security approaches used by the judicial branch, and documentation thereof are based on the NIST defined cybersecurity framework, and National Center for State Courts best practice recommendations.

The Supreme Court will use the auditor's recommendations in order to perform a review of existing documentation to identify gaps. Should the OCIO or the state develop a specified format for the reports designated in the NITC Standards, the Supreme Court could also consider adopting this model.

* * * * *

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 management, 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.

Pat Reding

Pat Reding, CPA, CFE
Assistant Deputy Auditor