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

October 6, 2022

Corey R. Steel, State Court Administrator
Nebraska Supreme Court
Nebraska State Capitol, Suite 1213
Lincoln, Nebraska 68509

Dear Mr. Steel:

This letter is provided pursuant to AICPA Auditing Standards AU-C Section 265.A17, which permits the early communication of audit findings due to their significance and the urgent need for corrective action. The audit work addressed herein was performed as part of the fiscal year ended June 30, 2022, Annual Comprehensive Financial Report (ACFR) audit. This communication is based on our audit procedures through June 30, 2022. Because we have not completed our audit of the fiscal year 2022 ACFR, additional matters may be identified and communicated in our final report.

In planning and performing our audit of the State's financial statements as of and for the year ended June 30, 2022, in accordance with auditing standards generally accepted in the United States of America, we considered the State's internal control over financial reporting (internal control) as a basis for designing the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

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.

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, and, therefore, material weaknesses may exist that were not identified.

We noted certain internal control or compliance matters related to the activities of the Supreme Court, 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.

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 were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, the auditor does not express an opinion on them. Responses have been objectively evaluated and recognized, as appropriate, in the letter. Responses that indicate corrective action has been taken were not verified at this time, but they will be verified in the next audit.

The following are our comments and recommendations for the year ended June 30, 2022.

1. Court Order Approval

The Judicial User System to Improve Court Efficiency (JUSTICE) application is the Supreme Court's case and financial management system for Nebraska trial courts. DOCKET is a module within JUSTICE used to issue court orders that are affixed with the Judge's signature. While the court orders issued through DOCKET contain the Judge's signature, access to issue orders through DOCKET is not restricted to only Judges. In order to access DOCKET, a user must have specific JUSTICE authorizations that are granted to Judges and other court staff. As a result, other court staff can create and issue orders affixed with the Judge's signature without formal documentation to support that the Judge approved the order.

Additionally, in some instances, the same court staff that can issue court orders through DOCKET may also have access to court receipts and be able to record non-monetary transactions (e.g., waiving fines) in JUSTICE.

A good internal control plan requires procedures to ensure that there is proper documentation of those who formally approved court orders.

The lack of such procedures increases the risk of an improper order being entered and not identified in a timely manner. Additionally, this absence of accountability could create a lack of segregation of duties because staff with the ability to issue court orders may also handle court receipts and waive fines.

A similar finding was noted during the previous audit.

> We recommend the Supreme Court implement procedures to ensure that each Judge's approval of orders is formally documented. We also recommend the Supreme Court review the impact that the current lack of such procedures may have on the segregation of duties at its courts.

Supreme Court Response: The Administrative Office of the Courts and Probation (AOCP) understands there is a risk related to the ability of someone other than the judge applying the judge's signature to an order within the DOCKET subsystem of JUSTICE, the court's case management system. This level of access is granted only to employees who work directly with the judges in and outside of the courtroom and only with the judge's approval and oversight. This electronic signature process is put into place to digitize and streamline the court process. Based on an evaluation of the level of risk, current IT priorities and resources, and a review of compensating controls and practices, the AOCP has determined that further action to significantly reduce the risk cannot be undertaken at this time.

2. JUSTICE Terminated User Access

During testing of terminated employees of State and local entities, it was noted that five of five terminated State users and one of one county user tested did not have their JUSTICE access removed in a timely manner, within three business days of termination of employment.

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. The JUSTICE team was not notified of any of the six terminated employees tested. The time between termination and employee access being removed ranged from 24 to 143 business days.

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 Information Systems and Organizations, Access Control 6 (AC-6), Least Privilege, states, in part, the following:

> *Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.*

A good internal control plan requires 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 not only inappropriate access to State assets and resources but also the unauthorized processing of transactions and changes.

A similar finding was noted during the previous audit.

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

Supreme Court Response: The AOCP will continue to work on and consider improvements in our termination process for internal and external JUSTICE users.

As noted in the past, a former employee would no longer have access to a computer authorized to connect to the state network. Since JUSTICE is not accessible from outside the state firewall, the AOCP contends that the risks from improper access are significantly reduced.

* * * * *

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 interim 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 suitable for any other purpose. However, this communication is a matter of public record, and its distribution is not limited.

Zachary Wells, CPA, CISA
Assistant Deputy Auditor