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 19, 2018

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, 2017, 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 14, 2017. 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.

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 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 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, 2017.

1. Implementer Access

During testing, we noted six user IDs, five contracted programmers, and one Office of the Chief Information Officer Applications Developer had move and checkout access to the Judicial User System To Improve Court Efficiency (JUSTICE) development, test, and production environments.

Nebraska Information Technology Commission (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 (December 2013), 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.*

Without proper and consistent segregation of duties in the change management process, changes to systems may be made without specific approvals. This could lead to data loss, loss of financial data integrity, and unintended system downtime.

A similar finding was noted during the previous audit.

> 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: In April of 2017, the OCIO confirmed that their employees' permissions to checkout objects in all environments had been removed. Additionally, in September of 2017, the Supreme Court began promoting changes under the OCIO's change management process. Changes are now staged by JUSTICE programmers weekly, notice is sent to the OCIO help desk, which creates a ticket in the Service Portal, and changes are then promoted by OCIO staff to production.

2. JUSTICE Terminated Users

The Supreme Court did not have an adequate process in place to ensure JUSTICE access was removed in a timely manner upon user termination. We noted 11 users still had access to JUSTICE after their termination dates. One of these users signed on to the JUSTICE AS/400 after his termination date. As of the date of testing, users retained access from 11 to 202 business days past their termination dates. Users had been employed by the Supreme Court (1), Sarpy County (1), the Department of Health and Human Services (5), and the State Patrol (4).

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.7.2, User Account Management, states, in relevant part, 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 periodic communication with outside agencies to ensure notification of terminations are received in a timely manner, and it also includes a process to ensure terminated users' access in JUSTICE is removed timely.

Failure to terminate user access to applications timely creates the opportunity for inappropriate access to State resources.

A similar finding was noted during the previous audit.

> We recommend the Supreme Court implement procedures to ensure a user's access to applications is removed immediately upon his or her termination.

Supreme Court Response: Under the current user agreement, external entities have an obligation to notify the Supreme Court of termination of an employee with access to the JUSTICE program. The Supreme Court reserves the right to deny access to the JUSTICE system to outside agencies that do not provide notice of terminated users. The Supreme Court will look to find ways of communication with outside agencies on a periodic basis to try to ensure terminated users' access to JUSTICE is removed in a timely manner.

3. JUSTICE New Users

For 3 of 24 new users tested, adequate documentation was not on file to support that JUSTICE access was appropriate.

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.7.2, User Account Management, states, in relevant part, 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 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.

A similar finding was noted during the previous audit.

> 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 Supreme Court will improve documentation of communication between JUSTICE staff and court supervisors authorizing differently levels of staff user access to JUSTICE.

* * * * *

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