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 29, 2016

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, 2015, 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 17, 2015. 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 (Agency) 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 Agency'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 internal control that we consider to be material weaknesses or significant deficiencies. However, material weaknesses or significant deficiencies may exist that were not identified.

In addition, we noted other matters involving internal control and its operation that we have reported to management of the Agency in a separate early communication letter pursuant to AICPA Auditing Standards AU-C Section 265.A17, dated November 2, 2015.

Draft copies of this letter were furnished to the Agency 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, 2015.

1. Security Settings

Nebraska Information Technology Commission (NITC) Standards & Guidelines, 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 re-authentication 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.

The Judicial User System to Improve Court Efficiency (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.

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 comment was noted during the previous two audits. Our prior audit recommended that the Agency set its re-authentication setting to a more reasonable level, such as 30 minutes or less. The Agency responded to this prior year recommendation as follows:

> *The inactivity timer is a system setting on the AS/400 and is controlled by the OCIO. This is not a JUSTICE program specific time-out setting. We have inquired with the OCIO as to whether or not this could be adjusted down to a shorter time frame, however the request was not acted upon because to do so impacts the Department of Motor Vehicles and the individual county agencies who are running programs on the AS/400's and is therefore not something the Supreme Court can determine.*

We recommend the Agency work with the Department of Motor Vehicles (DMV) and the Department of Administrative Services, Office of the Chief Information Officer (OCIO), to determine if a re-authentication setting for the JUSTICE application and applicable DMV applications could be set to a more reasonable level, such as 30 minutes or less.

Agency Response: 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.

2. JUSTICE Change Management Procedures

NITC Standards and Guidelines, Information Security Policy 8-101, 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.

In our review of the change management process of the JUSTICE application, we noted that the change management documentation system, Bug Tracker, utilized by the Agency is not directly tied to actual changes placed into production within Implementer, a tool used to track and implement changes to JUSTICE by the 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 end June 30, 2015, from Implementer. We selected 10 days for testing; from those 10 days, we selected one request number per day. For 2 of 10 changes, we were unable to trace the actual change made in Implementer to the Agency's change management documentation system, Bug Tracker, as no service requests were generated for these changes. Additionally, there was no review of actual changes made by the OCIO programmers as reflected in Implementer to ensure all changes made were appropriate and authorized by the Agency.

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 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 Agency periodically obtain and review a report from Implementer of JUSTICE changes from the OCIO to ensure changes made were appropriate and authorized.

Agency Response: The Administrative Office of the Courts will work with the OCIO to obtain a periodic report of Implementer changes to the JUSTICE program, and to determine what methods are available to tie Implementer changes to Bug Tracker change documentation.

3. JUSTICE Terminated Users

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 requires that terminated user access be removed timely.

The Agency did not have an adequate process to ensure user JUSTICE IDs were disabled or deleted in a timely manner after an individual's termination. For 6 of 10 deleted JUSTICE IDs tested, the IDs were not deleted timely (within three business days of the user's termination). The time it took to remove access ranged from 4 to 36 business days.

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

> We recommend the Agency implement procedures to ensure user access is disabled or deleted within three business days of a user's termination.

Agency Response: The Administrative Office of the Courts will continue to review the process for terminating JUSTICE users with the goal of achieving timely terminations.

* * * * *

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 Agency 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 Agency.

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

Don Dunlap, CPA
Assistant Deputy Auditor