NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

Mike.Foley@nebraska.gov
PO Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
www.auditors.nebraska.gov

December 16, 2014

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

Dear Mr. Steel:

We have audited the basic financial statements of the State of Nebraska (State) as of and for the year ended June 30, 2014, 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, and have issued our report thereon dated December 16, 2014. 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 for the purpose of expressing our opinions on the basic 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 and, therefore, material weaknesses or significant deficiencies may exist that were not identified.

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, 2014.

1. Security Settings

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.5.4, Clear Screen, states:

> *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 protection 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 requires a user to re-authenticate to the AS/400 after four hours of inactivity. While the NITC Standard 8-101 does not indicate what the "predetermined period of inactivity" should be, four hours does not seem reasonable and in-line with the intent of the Standard to prevent unauthorized access to information.

A similar comment was noted during the previous audit.

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.

> We recommend the Agency set its re-authentication setting to a more reasonable level, such as 30 minutes or less.

Agency Response: 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.

2. Backup Procedures

NITC Standards & Guidelines, Information Technology Disaster Recovery Plan Standard 8-201, Section 1, states, in part:

> *Each agency must have an Information Technology Disaster Recovery Plan that supports the resumption and continuity of computer systems and services in the event of a disaster. The plan will cover processes, procedures, and provide contingencies to restore operations of critical systems and services as prioritized by each agency.*
>
> *The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency. The following elements, at a minimum, must be included:*
>
> - *Identification of critical computer systems and services to the agency's mission and business functions.*
> - *Critical systems and services preservation processes and offsite storage strategy and methods to protect storage media . . . .*
> - *Annual plan review, revision, and approval process.*

Additionally, NITC Standards & Guidelines, Information Technology Disaster Recovery Plan Standard 8-201, Section 5.2, Agency and Institutional Heads, states:

> *The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs consistent with this standard. The authority may delegate this responsibility but delegation does not remove the accountability.*

The APA noted 35 of 93 counties store JUSTICE data on a consolidated server with adequate backup procedures. The APA tested 4 of 58 counties with their own JUSTICE server and backup procedures. Two of the four counties tested, did not store backup tapes at an offsite location.

A similar comment was noted during the previous audit.

When backup tapes are not stored offsite, there is an increased risk for the loss of data or prolonged system downtime.

> We recommend the Agency require counties to store backup tapes offsite to ensure effective data retention. Additionally, we recommend the Agency continue to work toward the consolidation of servers.

Agency Response: Server consolidation was put on hold temporarily by the OCIO after completion of Phase I. The state was looking to make a change to its backup server system location, and the OCIO was contemplating making the move before setting up the new consolidated server required for Phases II and III. However, they have decided to move forward again now, and AS/400 consolidation is scheduled to begin again in the next several weeks. The completion of Phase II and III of the migration will bring the JUSTICE program and associated data for all but the largest courts on to virtual servers housed at the 501 building. It is the AOC's expectation that in counties where it is the court office's responsibility to create backup tapes that these must be stored off site. The AOC will provide a formalized set of instructions.

* * * * *

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.

Philip Olsen, CPA, CISA
Audit Manager