NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

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

March 4, 2013

Brenda Decker, Chief Information Officer
Office of the Chief Information Officer
Department of Administrative Services
501 South 14th Street
Lincoln, NE 68509

Dear Ms. Decker:

We have audited the basic financial statements of the State of Nebraska (the State) as of and for the year ended June 30, 2012, in accordance with auditing standards generally accepted in the United States of America, and have issued our report thereon dated January 16, 2013. 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 Department of Administrative Services – Office of the Chief Information Officer (OCIO), 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 OCIO's management, are intended to improve internal control or result in other operating efficiencies.

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.

Additional findings and recommendations were reported to the management of the Department of Health and Human Services (DHHS) and the Department of Labor in separately issued letters relating to requests for access to the OnBase System.

Draft copies of this letter were furnished to the OCIO to provide them an opportunity to review the letter and to respond to the comments and recommendations included in this letter. 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 will be verified in the next audit.

Background

Neb. Rev. Stat. § 86-519 (Reissue 2008) created the Office of the Chief Information Officer (OCIO). The duties of the Chief Information Officer are defined by Neb. Rev. Stat. § 86-520 (Cum. Supp. 2012). Some of these responsibilities include: maintaining an inventory of technology assets including hardware, applications and databases, recommending policies and guidelines for information technology, advising the Governor and Legislature on policies affecting information technology, and monitoring the status of technology projects.

Neb. Rev. Stat. § 86-515 (Cum. Supp. 2012) created the Nebraska Information Technology Commission (NITC) which consists of nine members including the Governor of Nebraska or his or her designee. The duties of the NITC are defined by Neb. Rev. Stat. § 86-516 (Cum. Supp. 2012), and include adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. The NITC includes the following members:

- Lieutenant Governor Rick Sheehy, Chair – Governor's Designee (Resigned February 2, 2013)
- Dan Shundoff – General Public
- Pat Flanagan – General Public
- Lance Hedquist – Communities
- Dr. Daniel J. Hoesing – Elementary and Secondary Education
- Mike Huggenberger – General Public
- Dr. Doug Kristensen – Postsecondary Education
- Donna Hammack – General Public
- Brad Moline – General Public
- Sen. Dan Watermeier – Ex officio, nonvoting member

The OCIO works with the NITC to ensure cost-effective and efficient use of State resources and investments in information technology. The OCIO assists NITC and its councils in preparing a statewide technology plan and strategies for using information technology.

All State agencies are required to be in compliance with such NITC standards and guidelines, unless they request and are approved for a waiver of the standard or guideline from the technical panel, or are noted as being specifically excluded in policy. The OCIO and NITC work closely with State agencies to meet their respective statutory requirements.

The State of Nebraska entered into a contract with eDocument Resources LLC, a licensed Hyland Software reseller, for the period of September 21, 2010, through September 20, 2015. The contract included the purchase and maintenance of an Enterprise Content Management (ECM) software solution. The contract as of December 31, 2012, totaled $8,225,370. The ECM software is a product from Hyland Software Inc. called OnBase. OnBase version 11 was in use during the audit period. The OCIO plans on implementing OnBase version 12 in April 2013.

To recover the cost of the software and maintenance, the OCIO charged agencies utilizing OnBase a monthly fee per user. The NITC adopted Standard 5-101 on April 11, 2012. The Standard states,

"1.1 State agencies managing content and creating workflow as described in Section 2 shall use the Enterprise Content Management System (ECM) that is provided through the Office of Chief Information Officer (OCIO). 1.2 Agencies must consider, through consultation with the OCIO, using the ECM's E-Forms software for any new electronic forms applications."

Section 4 of the Standard states,

"This standard does not apply to systems already in use by an agency, unless:

- *The agency intends to buy significant upgrades;*
- *The agency intends to buy a significant amount of new modules; or*
- *The agency intends to do a significant amount of custom development*

For guidance on these points, contact the OCIO."

The following are our comments and recommendations for the year ended June 30, 2012.

1. OnBase Workflow Execution

NITC Standard 8-101, Section 1, Operational Roles and Functional Responsibilities states, in part,

"Agencies that create, use or maintain information systems for the State of Nebraska must create and maintain an internal information security infrastructure that ensures the confidentiality, availability, and integrity of the State's information assets."

NITC Standard 8-101, Section 2, State of Nebraska Information states, in part,

"Agency information is an asset and must be protected from its creation through its useful life, and to its authorized disposal in accordance with the Records Management Act and your agency's retention schedule. State information must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use."

A good internal control plan includes implementing the principle of least privilege. That is the practice of granting users only the required access necessary to perform their normal job functions.

- The OnBase version in use during the audit period allowed users with view only access to execute workflow processes when using the "Unity" client. The Unity client, when installed on a user's machine, provided additional functionality not available using the Web client (accessing OnBase through a web browser).

- 5,903 DHHS IDs had access to the Payment Request Form, where a workflow could be executed through the Unity client. The global privileges user group granted to most users provided access to the Payment Request Form. Of the 5,903 users, 2,761 only had access to global access group(s) and employee evaluations. Per DHHS, employees utilize the web client for employee evaluations. DHHS staff utilized the Payment Request Form to submit requests for vendor payments. Those requests would then go through an approval process within OnBase and EnterpriseOne; the State's accounting system.

- OnBase lacked enterprise level controls to restrict users from using only the Web or Unity clients. In addition, users could not be restricted from only viewing documents that had been through all required workflow queues, if required.

When users with view only access have the ability to re-introduce documents into a workflow, there is an increased risk a duplicate payment to a vendor, employee, client, or citizen will be created in the State's accounting system.

> We recommend the OCIO adequately test version 12 of the OnBase software to ensure controls will be in place to prevent users with view only access from re-introducing documents into a workflow. We also recommend the OCIO work with DHHS to evaluate the Payment Request Form access assigned to nearly all DHHS employees and other political subdivision users, and remove access when it is not required.

OCIO's Response: During the version 12.0 upgrade, the OCIO and agencies have a plan to thoroughly test the OnBase Software to insure that controls are in place to prevent users with view only access from re-introducing documents into a workflow. The version 12 upgrade is currently scheduled for April 2013.

DHHS' Response: The Department (DHHS) allows any employee to present an invoice for payment using the Payment Request Form. The ability to request a payment is different than the ability to approve a payment.

2. Release Migration (Change Management)

NITC Standard 8-101, Section 9, System Development and Maintenance states, in 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 Standard 8-101, Section 7, Access Control states, in part,

> *"All individuals requiring special privileges (programmers, database administrators, network and security administrators, etc.) will have a unique privileged account (UserID) so activities can be traced to the responsible user. UserIDs must not give any indication of the user's privilege level, e.g., supervisor, manager, administrator, etc."*

NITC Standard 8-101, Section 3, Personnel Accountability and Security Awareness states, in 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.

An OCIO contract developer was granted access to the MANAGER super user account and completed an OnBase project migration outside of the established release migration process. One of three DHHS releases tested was completed by the contractor. Supporting documentation (workflow queue history) showed the project was in an early phase of the release migration process (dev queue); however, we confirmed the project was in production and being used by DHHS.

When developers are allowed access to super user accounts, have access to migrate changes to the production environment, or perform changes outside of established procedures, there is an increased risk changes will occur that are not in agreement with management's intentions.

> We recommend the OCIO restrict OnBase developer access to non-production environments. We also recommend eliminating developer access to OnBase super user accounts and only provide access that ensures changes go through the established release migration workflow approvals before being promoted to production.

OCIO's Response: The Office of the CIO agrees with the recommendation to restrict OnBase developer's access to non-production environments. The OCIO will work with the agencies to review and remove "super user" accounts privileges.

3. Password Complexity

NITC Standard 8-301, Section 2.1, Password Construction requires users to follow these minimum password requirements:

- Must contain at least eight (8) characters
  - Must not repeat any character sequentially more than two (2) times
- Must contain at least three (3) of the following four (4):
  - At least one (1) uppercase character
  - At least one (1) lowercase character
  - At least one (1) numeric character
  - At least one (1) symbol

- Must change at least every 90 days
- Cannot repeat any of the passwords used during the previous 365 days.

A good internal control plan includes utilizing system parameters to enforce password rules that require users to comply with NITC standards.

OnBase uses Microsoft's Active Directory for authentication. Active Directory password complexity rules are not flexible enough to meet all the requirements of the NITC password standard. Active Directory cannot prevent the use of characters being repeated sequentially more than two times.

Strong complex password settings reduce the risk of an unauthorized user gaining access to confidential information and key financial data.

> We recommend the OCIO implement password complexity requirements to ensure user compliance with NITC requirements. When systems are not capable of forcing users to comply with NITC requirements, we recommend requesting a waiver for NITC's consideration.

OCIO's Response: The Office of the CIO will continue to work with agencies to ensure NITC compliance and/or exceptions will be documented through the NITC process.

4. DHHS Terminated User Access

NITC Standards and Guidelines, Information Security Policy 8-101, Section 7, Access Control states, in part,

> *"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…Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges."*

A good internal control plan includes a process to terminate users access in a timely manner.

During a review of user access, we noted one terminated user whose access was not removed in a timely manner.

When access to networks and applications is not terminated timely, it creates the opportunity for unauthorized processing of transactions.

> We recommend the OCIO ensure terminated users access be removed within three business days.

OCIO's Response: The Office of the CIO will continue to work with agencies to establish a review schedule of all users and the access to applications and formalize a process to grant and remove access to these applications.

DHHS' Response: The Department has reviewed the circumstances regarding the terminated user's access. The terminated employee's access did not allow the employee to change anything in the system without the employee being physically on the Department's premises. While the user's access was not terminated until twelve days after the termination date, the employee's badge was taken from the employee on the date of termination thus the employee was unable to enter the Department's premises.

* * * * *

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 OCIO 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 OCIO.

This report is intended solely for the information and use of the OCIO, the Governor and State Legislature, others within the OCIO, 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 report is a matter of public record and its distribution is not limited.

SIGNED ORIGINAL ON FILE

Philip J. Olsen, CPA, CISA
Audit Manager

SIGNED ORIGINAL ON FILE

Pat Reding, CPA, CFE
Assistant Deputy Auditor