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

May 11, 2012

Brenda Decker, Chief Information Officer
Office of the Chief Information Officer
Department of Administrative Services
501 South 14th Street
Lincoln, NE 68508

Dear Ms. Decker:

In connection with our Federal Office of Management and Budget (OMB) Circular A-l33 audit (the Single Audit) of the State of Nebraska for the fiscal year ended June 30, 2012, and the audit of the Comprehensive Annual Financial Report (CAFR) of the State of Nebraska (State) for the fiscal year ended June 30, 2012, we performed testing of the State's Information Technology (IT) internal control procedures for select applications administered by the Chief Information Officer (CIO) and State agency management. These systems support financial reporting and disclosures for the State.

The design and operating effectiveness of applicable computer controls were tested through internal control procedures. We discussed, confirmed, and observed controls with each respective agency's management. The procedures performed related to computer operations, information security, and change management consisting of a combination of inquiry, corroboration, observation, and re-performance. Interfaces significant to financial reporting were also selected for testing.

We noted certain internal control or compliance matters related to the activities of the IT Systems tested or other operational matters that are presented below. The specific confidential details and information were provided separately to each respective agency's management and your office, and is intended to improve internal control or result in other operating efficiencies.

The Office of the Chief Information Officer (OCIO) was provided the opportunity to respond to the comments and recommendations included in this letter, and their formal responses have been incorporated. Responses by the OCIO have been objectively evaluated and recognized.

Background

Neb. Rev. Stat. § 86-519 (Reissue 2008) created the OCIO. The duties of the Chief Information Officer are defined by Neb. Rev. Stat. § 86-520 (Cum. Supp. 2010). 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. 2010) 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. 2010) and include adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. The Commission includes the following members:

- Lieutenant Governor Rick Sheehy, Chair – Governor's Designee
- 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
- Dr. Janie Park – General Public
- Trev E. Peterson – General Public
- Sen. Galen Hadley – 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 following is a high-level overview of the applications included in our testing:

Department of Administrative Services (DAS):

- ***Oracle's JD Edwards EnterpriseOne 9.0 (EnterpriseOne)*** – This application is responsible for processing the financial, human resource, and procurement data business processes for the State of Nebraska. There are extensive interfaces with other State applications.

- ***CSB & PAC*** – applications utilized by DAS to track and bill telecommunications and Information Management (IM) Services billings to State agencies and other related entities.

- ***Kronos*** – Kronos is an attendance collection software system used by the Department of Correctional Services and the Department of Health and Human Services to record employee hours. Employee hours entered in Kronos interface with EnterpriseOne.

Department of Health and Human Services (DHHS):

- ***Children Have A Right To Support (CHARTS)*** – CHARTS is used for statewide Child Support Enforcement (CSE). Processes include case initiation, location, establishment, case management, enforcement, financial management, and State/Federal reporting. There are extensive interfaces with other State and Federal organizations, including EnterpriseOne.

- ***Nebraska Family Online Client User System (NFOCUS)*** – The NFOCUS application is used to automate benefit/service delivery and case management for over 30 DHHS programs. NFOCUS processes include client/case intake, eligibility determination, case management, service authorization, benefit payments, claims processing and payments, provider contract management, interfacing with other State and Federal organizations, and management and government reporting. Payments processed through NFOCUS interface with EnterpriseOne.

- ***Medicaid Management Information System (MMIS)*** – This application supports the operation of the Medicaid program which is Federally-regulated, State-administered, and provides medical care and services. The objective of MMIS is to improve and expedite claims processing, efficiently control program costs, effectively increase the quality of services, and examine cases of suspected program abuse. MMIS claim payments interface with EnterpriseOne.

- ***Home Energy Assistance (HEA)*** – This application supports the Federally-funded Low Income Home Energy Assistance Program (LIHEAP). For qualified households, the Home Energy application stores the case information and generates energy assistance payments to both clients and providers. HEA payments interface with EnterpriseOne.

- ***Women, Infants, and Children (WIC)*** – This application is used to determine client eligibility and to print food instruments for the Special Supplemental Nutrition Program for WIC.

- ***Coordinating Options in Nebraska's Network Through Effective Communication and Technology (CONNECT)*** – Users access the CONNECT application through the State's portal. Individual users access to the application is controlled by the Access Restriction by Granular User Services (ARGUS) application. DHHS programs that utilize this application include the Early Development Network, the Aged and Disabled Waiver, the Centers for Independent Living, the Area Agencies on Aging, Respite Services, the Medically Handicapped Children's program, and the Disabled Persons and Family Support Services. The information entered into the system is utilized for numerous activities such as; tracking, authorizations, notifications, data, quality assurance, and payment to contracted services coordination agencies for services coordination. Some CONNECT payments interface with EnterpriseOne.

- ***Medicaid Drug Rebate*** **(*MDR)*** – The MDR application is used to create invoices for drug rebates received from the drug manufacturer and tracks the corresponding receivables for the invoicing. MDR interfaces with MMIS to receive claims data to calculate rebateable units and with the Centers for Medicare and Medicaid Services (CMS) to receive rebate amounts per National Drug Code (NDC) to create amounts for invoicing. MDR also sends utilization of NDCs to CMS.

Nebraska Department of Education (NDE):

- ***Grants Management System (GMS)*** – This application is used by outside users to apply for grant funds and by NDE to approve and process payments for grant funds. Grant payments made to pre-selected school districts are interfaced with EnterpriseOne through a separate process.

- ***Quality Employment Solutions through Teams (QUEST)*** – QUEST is utilized by Vocational Rehabilitation staff to track all expenses paid to assist physically and/or mentally disabled persons in locating jobs. It includes aid to complete school, help purchase dress clothes, set up interviews, etc. QUEST payments interface with EnterpriseOne.

- ***Disability Determination System (DDS)*** – This application serves as a customer resource manager and information tracking system for payments to medical practitioners for information they provide to the social security administration pertaining to pending disability claims. DDS payments interface with EnterpriseOne.

- ***Child Nutrition Program (CNP)*** – This application is used by NDE to help administer the National School Lunch Program, Summer Food Service Program, Child and Adult Care Food Program (CACFP), including processing program claims and applications. CNP payments interface with EnterpriseOne through a separate process.

Department of Labor:

- ***Tax Management System (TMS)*** – TMS records daily transactions regarding employer Unemployment Insurance (UI) accounts.

- ***Benefits Payment System (BPS)*** – This application processes payments to eligible claimants for unemployment insurance and accounts for all overpayment collection activities.

- ***NEworks*** – This application is leased from a third party vendor, used by the Department of Labor to manage, track, and determine eligibility for individuals for various Federal grants. The application also serves as a self service tool for job seekers and employers.

Department of Motor Vehicles (DMV):

- ***Vehicle Titling and Registration (VTR)*** – This application was developed by the Department of Motor Vehicles to provide an overall system to be utilized by the counties in vehicle titling and registration.

- ***Traffic Safety Information (TSI) –*** This application was developed by the Department of Motor Vehicles to provide an overall system to be utilized by the counties to create, maintain, and update driver records.

- ***Motor Carrier System (MCS) –*** This application tracks motor carrier registration fees and taxes.

Nebraska Public Employees Retirement Systems (NPERS):

- ***Nebraska Public Retirement Information System (NPRIS)*** – NPRIS processes contributions from members and employers and prepares information for EnterpriseOne to print member benefit payments.

Department of Revenue:

- ***Revenue Mainframe Applications –*** The Department of Revenue utilizes the following mainframe applications to process tax filings: Fiduciary Income Tax Application (FIT), Sales & Use Tax Application (SCT), Sales & Use Tax Refund Application (STR), Corporate Income Tax Application (CTX), and Individual Income Tax Application (IIT). The Department of Revenue also utilizes the Electronic Tax Receipt (ETR) mainframe application to receive electronic funds transfer (EFT) tax payment records from the State's bank account. Each of these mainframe tax applications receive tax payment control records from the Nebraska Online Validation (NOV) application. An interface with EnterpriseOne issues the State payment of tax refunds.

- ***Revenue Oracle Applications –*** The Department of Revenue utilizes the following Oracle applications: General Processing System (GPS), Homestead Exemption, Motor Fuels Tax, Individual Income Tax E-file, and Validation Data Entry. The GPS application has several forms for some of the smaller taxes and fees that are remitted (such as cigarette tax, tire fee, litter fee, lodging tax, motorboat sales tax, drug tax, etc.). The Homestead Exemption application processes information submitted by taxpayers to determine if they are eligible for a property tax exemption. Motor Fuels Tax is the system for processing motor fuels taxes. The Individual Income Tax E-file is the system for processing individual income tax e-filing transactions which are then uploaded to the IIT mainframe application. Tax payments received via the mail are entered into the Validation Data Entry application and interfaced to NOV (mainframe) in order to create the control record.

- ***Enterprise Series System*** – Third party system used to track online and instant lottery ticket sales, results, and inventory.

- ***Internal Control System (ICS)*** – Third party system used to independently validate and balance online and instant lottery game results.

Department of Roads:

- ***Roads Billing System (RBS) –*** This application is utilized to process accounts receivables and related receipting for the Department of Roads.

Supreme Court:

- ***Judicial User System to Improve Court Efficiency (JUSTICE)*** – JUSTICE is an application used by the county and district courts to record all financial and case activity.

State Treasurer's office:

- ***KidCare*** – The KidCare application supports child support payment processing, including receipts and disbursements for over 100,000 child support payments to custodial parents each month.

- ***Wagers*** – The Wagers application maintains information regarding unclaimed property remitted to the State of Nebraska and pays claims for specific property held.

The following are the comments and recommendations for the year ended June 30, 2012, related to the State of Nebraska IT Systems controls. It should be noted this letter is critical in nature since it contains only our comments and recommendations on the areas noted for improvement.

COMMENTS AND RECOMMENDATIONS

1. Developer Access to Production Environment

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 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. At a minimum the audit of security must remain independent and segregated from the security function."

Good internal control includes restricting access to information resources based upon job responsibilities to help enforce proper segregation of duties and reduce the risk of unauthorized system access. Programmers should generally be limited to accessing only the information specifically required to complete their assigned systems development projects, and expressly prohibited from altering production data and production software.

- Three QUEST application developers and database administrators, two DDS application developers, and one Social Security Administration DDS contracted developer at the Department of Education had full access to the production environments. When QUEST changes are moved to the staging environment an email notification goes out to the developers alerting them of changes that are ready for production. However, the notification is controlled by the developers and can be turned off.

A similar comment was noted in prior IT audits.

Application developers with access to the database and the production environments have the ability to circumvent the standard change control process and implement modifications that may be inconsistent with management's intentions and could result in unauthorized changes to data.

> We recommend the Department of Education implement controls to ensure application changes are approved and documented. This includes implementing a segregation of duties in the change management process when migrating changes to production environments. If a segregation of duties cannot by maintained due to staff size, we recommend implementing compensating controls. Compensating controls may include reviewing audit logs, code changes, or automatic notifications to identify all changes made to the production environment.

OCIO's Response: The Office of the CIO will continue to work with the Department of Education to resolve the internal control issues identified and ensure the production environments are protected from unauthorized changes. Additionally, the Department of Education offered the response below:

The Department of Education and DDS responded: DDS - We are not contesting this finding and are planning no action on this item. VR (Quest) - Many limitations of the existing QUEST database system will be addressed by the implementation of a replacement system, QE2. At the implementation point, a Change Management Committee will be established to evaluate, authorize, and verify all changes to the data system. Unlike the current system, QE2 will have a separate server test environment for comprehensive testing and evaluation of proposed changes.

2. Access Commensurate with Job Responsibilities

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

Good internal control includes utilizing logical access controls to ensure user access is commensurate with their job responsibilities.

- We noted 3 of 91 mainframe user IDs with special attributes did not require the access based on their job responsibilities. The users were accountants or program managers whose agency had a separate help desk function for assigning user access or resetting user passwords.

- The established DHHS process for assigning NFOCUS access to users was not being followed. The NFOCUS Access Request Checklist was not properly completed for 4 of 5 users tested. The most current checklist could not be located for 2 of the users. For the third user, the job activities indicated on the checklist did not match the profiles assigned to the user. The fourth checklist had no job activities marked, but the user was still assigned profiles.

- There was no documented review of users with the ability to assign roles in ARGUS, which included individuals with super user access. ARGUS controls access to the Department of Health and Human Services CONNECT application.

- 234 user IDs with access to the Department of Motor Vehicles MCS application had not logged into the application in more than six months. 119 of those users had never logged into the application.
- 202 user IDs with access to the Department of Motor Vehicles VTR application had not logged into the application in more than six months. 35 of those users had never logged into the application.

- Two OCIO staff members had the ability to develop, approve, and promote changes to the DMV mainframe applications and did not need the access on a regular basis.

- Five employees from the Department of Education had the ability to approve both CACFP applications and claims in the CNP application.

- One Department of Health and Human Services user, employed by an external organization, did not require elevated CHARTS database access.

- The activation code allowing Department of Education staff level access to the GMS application was the same for each user and was not changed on a periodic basis. In addition, policies and procedures had not been established to document staff level user provisioning for the GMS application.

A similar comment was noted in prior IT audits.

Users improperly granted the ability to make changes to system security parameters may result in unapproved changes being implemented. If such access is not implemented and configured properly, business cycle controls may be ineffective. When users are granted inappropriate access, significant information resources may be modified inappropriately, disclosed without authorization, and/or unavailable when needed. When an individual has access beyond what his or her job responsibilities require, there is an increased risk for unauthorized changes or transactions that could result in the loss of State funds. Without periodically changing the activation codes allowing access to an application, there is an increased risk users may gain unauthorized access through the utilization of a single access code.

We recommend all application owners review a list of users on a periodic basis to verify access levels are appropriate based on job responsibilities of the employees. We also recommend developing procedures for identifying and removing inactive user IDs that are no longer needed.

OCIO's Response: *The Office of the CIO will continue to work with the agencies identified to establish a review schedule of all users of applications to verify access levels are appropriate. The OCIO will continue to refine our internal process to review mainframe access at least annually to ensure that access levels are appropriate. Additionally, individual agencies responses are listed below:*

The Department of Health and Human Services responded: CHARTS access that was found was subsequently removed 4/5/2012. DHHS is developing a process to review staff access/user profiles for applications. DHHS internal annual review process for access is being updated to initiate scheduled annual reviews by DHHS Service Area and Division. Annual reviews will be initiated and coordinated by the DHHS IT Security Administrator. Refresher training will be scheduled for all managers and supervisor from business units with access to N-FOCUS once the annual review procedure updates are published. Argus now stores the history of who gives what role to a user and when. Connect has added a table to log the assignment of roles. DHHS is developing a process to complete annual reviews by DHHS Service Area and Division to review user access.

The Department of Motor Vehicles responded: The Department of Motor Vehicles does perform periodic checks of user and access levels. The user ID's referenced above are local and state law enforcement ID's and system pass through ID's. The DMV removes user access when we are notified by the user agency that the employee is no longer with the state or when the user no longer requires the access to perform their job.

The Department of Education responded: CNP - The logic put in place to not allow access was an after the fact solution. This logic only kicks in if a change is made to a person's access on that screen. If someone already had access and no changes were made the logic would not be activated; thus, someone could have inappropriate access rights. For some reason the 2 claim screens were set to 'Neutral' which allowed access; however, the two screens have been reset to 'Claims' and also the Userids that were incorrectly set have been changed. GMS - The Portal Administrator will periodically send out reminders to the Collection Administrators, including GMS, for these administrators to check their NDE Staff users. These reminders will include instructions on how to get a list of all NDE Staff members that they are responsible for in their collection. They are able to identify and remove any NDE Staff members as they see fit. NDE HR notifies the NDE Portal Administrator as each NDE Employee leaves the department. Their collections are removed from their Portal account, and the account is disabled and closed. The activation codes that changes a Portal account into an NDE Portal account are single-use only. They are only valid for a single person, and for only a single use. Once used, no one can re-use the code, including the person who originally used the code.

3. 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."

Nebraska State Accounting Manual, AM-005, General Policies, Section 32 states, "Each agency shall have a documented procedure to immediately disable the ENTERPRISEONE ID of an employee who has terminated employment with the agency. It is the responsibility of the agency's authorized agent to request termination of the User ID from the computer system within five working days from the termination date…"

Good internal control includes a process to ensure terminated users' access is removed timely.

- For 18 of 25 terminated EnterpriseOne users tested, their access was not removed in a timely manner. Six of those IDs accessed EnterpriseOne after the user terminated.
- There was no process to ensure Department of Education (NDE) GMS district administrator accounts were removed in a timely manner in the event of termination. The school districts were responsible for informing NDE of terminated administrators; however, no one at NDE monitored or reviewed the accounts.
- One Department of Motor Vehicles employee who terminated in May 2008 still had active MCS and VTR IDs. Another employee who terminated in November 2010 still had an active MCS ID.
- The OCIO was not notified of a Department of Motor Vehicles employee who terminated with elevated mainframe access. As a result, the OCIO opened a help desk ticket and attempted to contact the employee in regard to their ID after the termination date. The Department of Motor Vehicles subsequently reassigned the ID to a new individual.
- The Department of Roads did not have procedures in place to remove terminated employees' access to the network in a timely manner.
- We noted nine Supreme Court employees and six County employees who had terminated, and their access to the JUSTICE application was not removed in a timely manner. In addition, four terminated individuals' access had been removed from the JUSTICE application; however, they still had an active AS/400 ID.
- For 1 of 22 Department of Health and Human Services terminations tested, the employee's network and application access was not removed in a timely manner after the user's termination. Another employee's MMIS access was not removed after their termination in July 2011.

- For 1 of 20 terminations tested from a Department of Health and Human Services external contractor, access to MMIS was not removed after their termination in April 2011. DHHS relied on the external entities to notify them of terminated users, and did not perform a regular review of external users to ensure user access was appropriate. DHHS did maintain a manual listing of MMIS external users; however, the list was not kept current.

- The Department of Correctional Services did not remove KRONOS access for five terminated employees in a timely manner.

- One Department of Revenue vendor employee terminated in September 2011; however, the user's network access had not been removed as of March 2012. A periodic review of vendor accounts was not being performed.

A similar comment was noted in prior IT audits.

When access to networks and applications is not terminated timely, it creates the opportunity for inappropriate access to State resources. Such access may violate Federal laws regarding privacy issues.

> We recommend application owners review user access on a periodic basis to ensure access is appropriate. Additionally, a formalized process to remove access to both applications and networks should be established and followed. Terminated users access should be removed immediately. The creation, modification, and removal of a user's access should be documented and include a date stamp.

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

The Department of Education responded: There can only be a single district administrator for each district in the NDE portal. Thus, when a new administrator is added to a district, the departed administrator's access is removed from all Portal collections for that district, including GMS.

The Department of Motor Vehicles responded: The DMV believes that the users referenced above have been removed from the system.

The Department of Roads responded: We are developing a new User Access Request Application that we believe will help solve this problem. This application will utilize the SCSM software from Microsoft. We plan to have the application running by July, 2012. This still does not alleviate the issue with users not filling out the required form. To alleviate this issue we are reviewing monthly reports on unused userids' and contacting Divisions to see if they can be eliminated.

The Department of Health and Human Services responded: Changes were made to the Superior Group ID's on 4/5/2012 to meet NITC standards. Additionally, DHHS is currently reviewing and evaluating the DHHS password reuse policy.

The Department of Correctional Services responded: In response to previous year's findings, the Department of Correctional Services has developed a formalized access removal process, including periodic review of access. The formalized process includes documentation of access granted, and access removed, including date of action. The periodic review called for in that process was not conducted last year, but NDCS is committed to performing that task going forward.

The Department of Revenue responded: We agree with this recommendation. The Department of Revenue will develop and implement a procedure for conducting periodic reviews of vendor network accounts.

4. Shared IDs

NITC Standards and Guidelines, Information Security Policy 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."

NITC Standards and Guidelines, Information Security Policy 8-101, Section 3, Personnel Accountability and Security Awareness states, in part, "Each user must understand his/her role and responsibilities regarding information security issues and protecting state information. Access to agency computer(s), computer systems, and networks where the data owner(s) has authorized access, based upon the 'Principle of Least Privilege', must be provided through the use of individually assigned unique computer identifiers, known as UserIDs, or other technologies including biometrics, token cards, etc. Each individual is responsible for reasonably protecting against unauthorized activities performed with their UserID."

- The use of two system IDs used to support the EnterpriseOne application were not adequately monitored to ensure they were used only for approved purposes. A use log and system report identified when the IDs were used; however, an independent person was not reviewing the information.

- One ID with insert, update, and delete access to NPRIS production databases was shared by two Nebraska Public Employees Retirement Systems employees.

- The Auditor of Public Accounts (APA) noted 12 generic IDs were shared among users to gain access to the Supreme Court's JUSTICE application.

A similar comment was noted in prior IT audits.

Inadequate authentication procedures may lead to financial loss and operational damage through unintentional or deliberate unauthorized access, alteration, and use of information resources. Shared IDs make it difficult to identify the individual who accessed the computer system.

> We recommend eliminating all shared IDs when feasible to ensure individuals have a unique ID to make users accountable for transactions on computer systems. When it is not feasible to prevent the use of shared IDs, compensating controls should be in place to identify who and when the ID was used.

OCIO's Response: The Office of the CIO will continue to work with agencies to eliminate all shared IDs for accurate accountability. Additionally, individual agencies responses are listed below:

The Nebraska Public Employees Retirement System responded: The devuser ID was needed and created in October 2009 for the purpose of creating and connecting development workspaces for our OCIO developers, Melissa Kolm and Viji Pushkaran. The devuser ID is still needed in test, but is no longer needed in NPRIS Production. The devuser ID was deleted from NPRIS production February 10, 2012.

5. Password Complexity

NITC Standards and Guidelines, Password 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.

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

Password policies were not enforced to require users to meet the minimum requirements of the NITC standard above as follows:

- Several State agencies use Microsoft's Active Directory for network authentication, and in some cases access to applications. 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.

- The Department of Health and Human Services Active Directory settings were not sufficient enough to prevent users from reusing passwords from the previous 365 days.

- We identified three Department of Health and Human Services mainframe user IDs which did not force the user to change their password periodically.

- The Department of Education GMS Portal login used by school districts did not force a user to change their password periodically.

- The Department of Motor Vehicles Windows, VTR, and MCS applications did not force users to meet several NITC password requirements including length, complexity, and reuse of passwords. 32 MCS and 18 VTR users were not required to change their password periodically.

- The Supreme Court's JUSTICE application password settings required password lengths to be between five and eight characters.

A similar comment was noted in prior IT audits.

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

> We recommend password complexity requirements be implemented 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 the 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. We will also use the NITC State Government Council to create a working group to find a solution to the Microsoft Active Directory issue identified above. Additionally, individual agencies responses are listed below:

The Department of Education responded: The NDE Portal, the authentication system for GMS requires users to create and maintain passwords with a minimum character length of 8 and must contain at least 1 alpha and 1 numeric character. Users are prompted every 180 days to verify/change email and retain/change passwords.

The Department of Motor Vehicles responded: It is our understanding that the OCIO will be implementing the functionality that will enable and require that all passwords meet the NITC standard.

6. Standardized Change Management Process

NITC Standards and Guidelines, Information Security Policy 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 Standards and Guidelines, Information Security Policy 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."

Good internal control 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.

- QUEST database changes performed by the Department of Education were not formally documented or approved, and there was no documented review of database change logs.
- The Department of Motor Vehicles did not have formalized change management procedures in place to include a change request, test documentation, and management approval for all application changes, or for VTR and TSI database changes. There was also a lack of segregation of duties surrounding the DMV change management processes.

A similar comment was noted in prior IT audits.

Without proper and consistent change control standards, changes to systems may be made without specific approvals. Without adequate testing, system modifications may not function according to user requests or management's intentions. This could lead to data loss, loss of financial data integrity, and unintended system down time.

> We recommend a standardized change management process be developed and implemented for all application and systems changes. The process should include documented change requests, approvals, testing procedures, and approval to implement the change into production.

OCIO's Response: The Office of the CIO will continue to work with agencies to establish standardized change management processes of applications and system changes. Additionally, individual agencies responses are listed below:

The Department of Education responded: Concomitant with the establishment of a Change Management Committee, a formal request and authorization documents will be used for all changes. This will replace the current system of verbal requests and approvals. Authorized personnel will be able to view these documents on-line via a repository with wiki-like capabilities.

The Department of Motor Vehicles responded: The DMV IT Division works directly with Division Administrators. All database and application changes are performed only at the request of the Division Administrator that owns the data and process. All database and application changes are approved by the authorized division prior to implementation.

7. System Monitoring

NITC Standards and Guidelines, Information Security Policy 8-101, Section 7, Access Control, states in part, "Activities of information systems and services must be monitored and events logged to provide a historical account of security related events. Agencies will implement appropriate audit logs to record events, exceptions and other security-relevant events. The Agency Information Security Officer or designee will regularly review logs for abuses and anomalies."

Good internal control includes adequately monitoring computer systems to verify they are operating according to management's expectations.

- We noted 15 State employees with multiple EnterpriseOne IDs had the ability to prepare and/or post transactions. Ten of those users had the ability to prepare and post their own transactions using multiple IDs. Individuals with multiple IDs were not monitored by the Department of Administrative Services.

- The Department of Roads did not have security alerts set up for the Windows environment. The Department of Roads has obtained software to alert them of problems, but the alerts have not yet been fully configured. In addition, the RBS application did not have the capability to record which user completed each element of the accounts receivable and receipting process for subsequent review.

- For the Supreme Court's JUSTICE application, there was no documented review of database changes. The OCIO maintains the database logs; however, there was no periodic review performed to ensure all changes were approved and necessary.

A similar comment was noted in prior IT audits.

When users can prepare and post their own transactions, it creates an opportunity for the processing of unauthorized transactions. Without monitoring security violation reports unauthorized users could access sensitive financial data on the network and financial applications without being detected. Without monitoring system event logs there is an increase risk for damage to operating systems and physical hardware. Without monitoring database logs, there is an increased risk for unauthorized changes that may go undetected by management.

We recommend a periodic review of users who can prepare and post their own transactions. We also recommend performing a documented review of necessary system event logs, violation reports, and database logs to detect unauthorized events or system failures.

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. Additionally, individual agencies responses are listed below:

The Department of Roads responded: Concerning the issue about the Windows environment, we do have the SCOM software available and we are setting up the alerts. The issue with the RBS application will be resolved with an upgrade to the system. This project is in a hold status due to priority concerns of our business partners but we will begin addressing the issue beginning July, 2012.

8. Business Processes

Good internal control includes monitoring Legislative Bills affecting your agency to ensure appropriate changes to existing applications or databases are made prior to the effective date of such bills.

Good internal control also includes procedures to ensure all funds received reconcile to other system applications, and to ensure the correct exemption rates are used for garnished wages.

- A Department of Motor Vehicles fee calculated by the VTR application was incorrect based on the calculation procedures noted in Neb. Rev. Stat. § 60-3,190 (Supp. 2011). VTR calculated the fee based on DMV's rules and regulations which appear to be in conflict with State Statute. VTR calculated a $5 fee for 14 year old or older vehicles and per Statute the fee should be $7.

- The Supreme Court did not reconcile the number of paid JUSTICE case searches through Nebraska Interactive to the number of searches performed according to the JUSTICE application. The JUSTICE application currently does not count the number of searches performed through Nebraska Interactive.

- The Department of Motor Vehicles did not reconcile the number of record searches noted by Nebraska Interactive to the number of searches performed according to the VTR application. The VTR application currently does not count the number of searches made on the application. The DMV receives money for searches performed through Nebraska Interactive.

- The Department of Administrative Services did not use the correct tables within EnterpriseOne when calculating employee wage garnishments for delinquent State taxes. They had been using the Federal exemption amounts which did not agree to the Nebraska rates.

A similar comment was noted in prior IT audits.

When applications are not designed or updated to meet State statute requirements, and a lower fee than is required is collected, the State loses revenue. When a reconciliation of searches is not performed there is an increased risk the agency is not receiving all funds due to them. When the correct table for calculating garnishments for delinquent State taxes is not used, the employee's pay is calculated incorrectly.

> We recommend the Department of Motor Vehicles update the VTR application as needed to comply with State Statute. We also recommend the Supreme Court and DMV implement procedures to reconcile search activity to funds received from Nebraska Interactive. We also recommend the Department of Administrative Services work with Oracle to add an additional table for the State exemptions for State tax levies.

9. Business Continuity

NITC Standards and Guidelines, Information Technology Disaster Recovery Plan Standard 8-201, Section 1.0 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 Disaster Recovery Plan for Information Technology may be a subset of a comprehensive Agency Business Resumption Plan which should include catastrophic situations and long-term disruptions to agency operations."

IT Governance Institute's Control Objectives for Information and Related Technology (COBIT) 4.1 states, in part, "The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilizing offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimizes the probability and impact of a major IT service interruption on key business functions and processes."

- The DMV Motor Carrier Services application processed the collection of more than $87 million in calendar year 2010. The contracted programming support for the application consisted of one individual with both the business knowledge and programming skill set required to support the application. DMV had no backup plan should the programmer become unavailable. DMV stated they would require programming assistance from the OCIO and possibly former DMV employees, but the business knowledge could take years to acquire. This was also an issue for VTR, TSI, and a TSI sub-application.

- Backup tapes at each of the 93 County Courts were generated; however, there was no requirement to store them off-site.

- The Department of Revenue did not have a disaster recovery plan in place for their Oracle applications.

A similar comment was noted in prior IT audits.

When tested business continuity plans are not in place and tapes are not maintained off-site, there is an increased risk for the loss of data or prolonged system down time.

> We recommend State agencies develop complete formalized business continuity plans, which includes testing and maintaining backup tapes off-site to ensure effective data retention. We also recommend the Department of Motor Vehicles evaluate the risks associated with relying on one individual to provide application support, and consider training additional staff to support the MCS, VTR, and TSI applications.

OCIO's Response: The Office of the CIO will continue to work with agencies to establish formalized business continuity plans with effective data retention testing and storage. Additionally, individual agencies responses are listed below:

The Department of Motor Vehicles responded: The DMV is aware of the risk associated with not having duplicative staff for each functional area. During the 2012 legislative session, additional FTE was granted that will be used to reduce that risk. It should also be clarified that the DMV does perform daily, weekly and monthly back-ups of all data. These backups are performed across the state network from the Nebraska State Office Building to the OCIO facility and are subsequently moved to tape and off site.

The Department of Revenue responded: The Department of Revenue's Oracle servers have been moved to the OCIO VMware / Storage Area Network (SAN) environment as of April 14, 2012. Those servers are being backed up and the data resides on the OCIO SAN which is replicated to an offsite disaster recovery location. They are also covered by the OCIO I.T. disaster recovery plan because they are responsible for administering and maintaining the VMware environment and the SAN. However, backups and disaster recovery planning for Department of Revenue assets will continue to be a shared responsibility between Revenue and the OCIO, and the Department of Revenue will continue to work on developing an up-to-date I.T. disaster recovery plan.

10. Edit Checks

Good internal control includes the use of automated edit checks when possible to create segregation of duties and to prevent data entry errors. Edit checks should be tested to ensure they are functioning properly.

- The APA identified transactions posted in EnterpriseOne without an object account code. In addition, one agency posted transactions to an account code and then subsequently changed their chart of accounts structure causing the general ledger and budget status to disagree. Appropriate edit checks or business rules were not in place at the time to prevent those errors.

- Two of 15 CNP edit checks tested at the Department of Education did not set as expected.

- The Department of Health and Human Services HEA application does not include an edit check to ensure that only one member of the household is receiving energy assistance payments.

- The Department of Health and Human Services NFOCUS application contained a service authorization edit check that could be overridden, and there was no data available to determine how often the edit was overridden, or who performed an override. In addition, DHHS was unable to explain what circumstances would require the edit to be overridden.

Without appropriate edit checks in place, tests to ensure edits are functioning properly, and a review of overrides, there is an increased risk for accounting and reporting errors, exorbitant or fraudulent service authorizations and/or claim payments.

> We recommend State agencies work to ensure proper edit checks are in place; and perform periodic reviews to ensure that these edit checks are functioning properly and not being inappropriately overridden.

OCIO's Response: The Office of the CIO will continue to work with agencies to establish effective edit checks. Additionally, individual agencies responses are listed below:

The Department of Education responded: Business rule 238 is working; however, it is not setup correctly in the error code maintenance table to display correctly. The error code maintenance screen has been reset for error code type 238 to an 'I' to ensure it displays correctly on the claim screen. What is occurring is the 'I' looks correct on the maintenance screen but in reality it is not. Now that this is done it will display correctly in the errors list for the claim. No coding changes were needed for this resolution. Error Code 167 had been removed in FY 2010 since the claim no longer must have the signature of an authorized signer.

The Department of Health and Human Services responded: There is an N-FOCUS System Change Request documented to add additional functionality to the Service Authorization edit overrides as recommended. The SCR has a Target Release Date of November 11, 2012. The LIHEAP program will be moved into N-FOCUS with the July 8, 2012 release. All members of the energy assistance household will be added to the LIHEAP program case. There will be alerts generated when there is potential duplicate program participation.

11. Physical Security Access

NITC Standards and Guidelines, Information Security Policy 8-101, Section 5, Physical and Environmental Security states, in part, "To detect and prevent unauthorized access attempts in areas within facilities that house sensitive or confidential information, where possible, agencies must utilize physical access controls designed to permit access by authorized users only that identify, authenticate and monitor all access attempts to restricted areas within agency facilities."

Good internal control includes datacenter access controls to restrict access to individuals who do not require access to complete their job functions.

- During our review of user ID badges with access to an OCIO datacenter, we noted 7 of 157 badges were assigned to individuals whose access appeared inappropriate. One individual had terminated and six did not require the access to perform their job functions.

- Two of 43 badges tested with access to a Department of Health and Human Services datacenter were not appropriate. One badge was a generic ID owned by the Department of Administrative Services Building Division and one ID belonged to a terminated DAS Building Division employee. The employee's badge was used to access the datacenter 102 days after his termination.

Without procedures in place to adequately remove terminated employee access and periodically review access to a datacenter, there is an increased risk of inappropriate or unauthorized individuals accessing the State's physical IT resources.

> We recommend agencies work to review access to their datacenter(s) periodically and limit access to individuals who require it to perform their job functions.

OCIO's Response: The Office of the CIO will continue to work with the Nebraska State Patrol and state agencies to ensure that physical security to the State data center and other IT environments appropriately restrict physical access. Additionally, individual agencies responses are listed below:

The Department of Health and Human Services responded: DHHS is working with the State Building Division (DAS) on this issue. The badge is being de-activated. DHHS has requested a quarterly access list from Support Services which will include all access to the restricted area, as well as a current list of all users authorized to access that area. This list will be used to regularly review access.

* * * * *

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 State of Nebraska IT Systems gained during our work to make comments and recommendations that we hope will be useful to you.

This letter is intended solely for the information and use of the CIO, the Governor and State Legislature, Federal awarding agencies, and management of the State of Nebraska. However, this letter is a matter of public record and its distribution is not limited.

Sincerely,

SIGNED ORIGINAL ON FILE

Philip Olsen, CPA, CISA
Senior Auditor-In-Charge

Pat Reding, CPA, CFE
Assistant Deputy Auditor