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

August 12, 2011

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:

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, 2011, and the audit of the Comprehensive Annual Financial Report (CAFR) of the State of Nebraska (State) for the fiscal year ended June 30, 2011, we performed testing of the State of Nebraska's Information Technology (IT) internal control procedures for select applications administered by the Office of the Chief Information Officer (OCIO) and State agencies' management. These systems support financial reporting and disclosures for the State of Nebraska.

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 that agency's management and your office, and is intended to improve internal control or result in other operating efficiencies.

The 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 Office of the Chief Information Officer (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 IT, advising the Governor and Legislature on policies affecting IT, and monitoring the status of IT 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. A representative from the OCIO serves on the technical panel.

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

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.

The OCIO and the NITC work closely along with State agencies, to meet their respected statutory requirements.

The following is a high-level overview of the applications included in our testing.

Department of Administrative Services:

- ***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.

Department of Correctional Services:

- ***Kronos*** – Kronos is an attendance collection software system used 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.

- ***Automated Computer Tracking System (ACTS)*** – The ACTS application supports the Every Woman Matters and Wise Woman Programs. These programs are Federally funded by the Center for Disease Control and Prevention (CDCP). They provide breast and cervical cancer and cardiovascular and diabetes screening to women ages 40-64. The application is used to determine program eligibility, manage client health records, calculate payments to providers, and create reports for the CDCP.

- ***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 to 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, including processing program claims and applications. CNP payments interface with EnterpriseOne through a separate process.

Nebraska Game and Parks

- ***Reserve America*** – This web based application is operated by a third party vendor, used by the public and the Nebraska Game and Parks Commission to make and track reservations for campsites and lodging at Nebraska State Parks.

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 DMV 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 DMVto 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 payment of tax refunds from the State.

- ***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 tax payers 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 system is 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.

Department of Roads:

- ***Project Finance Systems (PFS)*** – PFS is an application used by the Department of Roads to track the billings and receipts for road projects. PFS accounts for the establishment of road projects and tracks and allocates expenses to the correct funding source.

- ***Roads Payment System (RPS) –*** The Department of Roads utilizes RPS to process and track all payments to vendors. RPS interfaces all transactions with EnterpriseOne.

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

- ***General Ledger System (GLS) –*** This application is utilized to track financial information for the Department of Roads. The information per the General Ledger System is reconciled on a monthly basis to EnterpriseOne.

State Records Board:

- ***Nebraska Interactive*** – Nebraska Interactive has contracted with the Nebraska State Records Board to provide web hosting for Nebraska government sites, including the State's portal (www.nebraska.gov). Nebraska Interactive charges fees for online services that are split with State agencies.

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.

Following are the comments and recommendations for the year ended June 30, 2011, 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. All findings related to DMV can be found in more detail in the Calendar Year 2010 Attestation Report of the Nebraska Department of Motor Vehicles issued July 11, 2011.

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.

- Two application developers at the State Treasurer's office had administrator access to the Windows environment, the KidCare application, and the KidCare database.

- All QUEST application developers, two DDS application developers, and one Social Security Administration DDS contracted developer at the Department of Education had full access to his or her respective production environments.

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 developers be required to obtain approval prior to moving changes into production. Depending on the size of the department, developers may need access to the production processing environments; however, compensating controls should be established. The compensating controls may include reviewing audit logs 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 agencies identified to resolve the internal control issues identified and ensure the production environments are protected from unauthorized changes. Additionally, individual agencies responses are listed below:

State Treasurer's office Response: Administrative access has been removed for both application developers using the KidCARE application to change data. There has been an approval process in place for quite some time that requires the developers to obtain approval, have their changes tested and approval to move into production. There are compensating controls in place in the form of logs and reports that can be audited by management at any time.

Department of Education's Response: Due to limited staff, there are only two DDS IT specialists. It is not practical to restrict one to the test environment and the other one to the production environment as they need to serve as back-up for each other. The system maintains a log of changes and builds in production. The Social Security Administration is moving toward a nationally maintained system that will remove almost all local programming.

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. 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.

- We noted 6 of 109 active mainframe user IDs with special attributes did not require the access based on their job responsibilities. One of those IDs was assigned to run vehicle and license information for the Nebraska State Patrol, and was shared among the Auto Fraud Division staff. Four users were accountants or program managers whose agencies had a separate helpdesk function for assigning user access or resetting user passwords. One user worked in a department with a total of two mainframe IDs, and did not appear to need the ability to assign access or reset passwords.

- One DDS employee did not require the elevated security access she was assigned in the DDS application based on her job responsibilities. In addition, two DDS employees had second IDs created due to name changes; however, their original IDs were not deleted.

- 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.

- One active DHHS CONNECT user had super user access; however, the user no longer needed such access. This user was noted in the prior year IT report, but was not corrected. Access to the CONNECT application was controlled by the ARGUS application. There was no documented review of users with the ability to assign roles in ARGUS.

- Several DMV mainframe and AS/400 users had access which was not necessary to perform their job functions. Additionally, two OCIO employees could develop, promote, and approve changes to DMV's mainframe applications.

A similar comment was noted in prior IT audits.

When an individual has access beyond his or her job duties, 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 regular basis to verify access levels are appropriate based on job responsibilities of the employees.

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 establish a process to review mainframe access at least annually to ensure that access levels are appropriate. Additionally, individual agencies responses are listed below:

Department of Education's Response: The finding for DDS has been addressed and corrected.

Access to GMS applications (collections) by NDE staff is allowed based on the roles and responsibilities of the user as defined for each separate collection. The roles and responsibilities are defined and documented in the Portal which is the source of the activation codes. Individuals only have access in the GMS to the level needed to complete their job duties (roles and responsibilities).

It is true that some individuals have the same activation code. A primary example is one application that combines 8 grant applications. There are about 260+ applications and these are reviewed by 10 federal program staff (that include the directors of the 8 grants). This means that each of the program directors of these 8 grants must be able to access the consolidated applications that are assigned to other staff.

Applications (collections) in the GMS are, for the most part, not annual activities but ongoing or multi-year projects.

The following process was implemented as a result of this finding: The Portal Administrator sends periodic reminders to the collection or system administrator/owner to review the users with access and the level of access for each user.

Department of Motor Vehicles' Response: The DMV will review its password and user ID process for improvement where possible and necessary. The DMV will also institute an annual review of user authorization levels.

3. Dataset Access

NITC Standards and Guidelines, Information Security Policy 8-101, Section 7, Access Control states, in part, "The issuance and use of privileged accounts will be restricted and controlled. Processes must be developed to ensure that users of privileged accounts are monitored, and any suspected misuse is promptly investigated."

Good internal control includes limiting application developers to non-production datasets. Logical security tools and techniques should be used to define such access restrictions, including how and to whom the entity will limit the ability to view, use, or modify significant information resources.

The following was noted regarding access to production datasets for DHHS applications:

- One developer had alter access to production datasets for the CHARTS application. In addition, there was one shared on call user ID with alter access to the CHARTS production datasets.

- Four developers had alter access to production datasets for the MMIS application.

- Fifteen developers had alter access to production datasets for the NFOCUS application.

- Four developers had alter access to production datasets for the HEA application.

A similar comment was noted in prior IT audits.

Without a proper segregation of duties, application developers could circumvent the change control process and modify the production environment without testing or obtaining management approval for changes. The resulting changes may lead to difficulties in maintaining system functions, processing errors, or inaccurate and misleading financial information.

> We recommend management evaluate potential options to restrict application developers' access to the production environment. In the event access restrictions are not feasible, monitoring controls should be implemented to ensure all modifications to the production environment are appropriately approved and tested.

OCIO's Response: The Office of the CIO will continue to work with agencies to evaluate the potential options to restrict application developer's access to the production environment and create appropriate monitoring controls. Additionally, individual agencies responses are listed below:

Department of Health and Human Services' Response: DHHS has established a safeguard control to mitigate this risk. The monitoring controls are Biannual Alter Access User Reviews that are conducted by the application technical managers and the agency's HIPAA/Security manager in January and July of each year. This process began in 2010 and has continued. Results of the audits have been provided to the Auditor of Public Accounts. The process of using "on-call" rotation has been the only way the agency has been able to support off-hours emergencies. Budget is not available to have designated application developers for 24/7 support of the applications. The bi-annual review is a follow up to determine those listed are appropriate.

4. 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."

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

- For 17 of 25 terminated EnterpriseOne users tested, their access was not removed in a timely manner. Two of those IDs accessed EnterpriseOne after the user terminated. During our review of EnterpriseOne power user IDs with access to all objects, we noted 13 of the 36 IDs were not appropriate because they were no longer needed.

- Three Department of Correctional Services Kronos users had terminated; however, their access had not been removed.

- There was no process to ensure the Department of Education GMS district administrator accounts were removed in a timely manner in the event of termination. The school districts were responsible for informing the Department of Education of terminated administrators; however, no one at the Department of Education monitored or reviewed the accounts.

- The Department of Roads did not have procedures in place to remove terminated employees' access to the network in a timely manner. The Department of Roads is in the process of developing an application to address this issue.

- The Supreme Court did not remove access for terminated JUSTICE users in a timely manner. We noted 10 users who had terminated, but still had access to the system. In addition, it was noted that one terminated individual's access had been removed from JUSTICE; however, they still had an active AS/400 ID.

- Six State and 24 external contractor's access to NFOCUS was not removed in a timely manner after the users termination. One of the contractor IDs was used to access NFOCUS after the user terminated. The Auditor of Public Accounts (APA) noted three individuals from one contractor terminated on March 4, 2011. While the contractor notified DHHS by email of the terminations on March 4, 2011, their access was not removed by DHHS. The APA noted several users in NFOCUS were listed as active, but their LAN access had been terminated.

- One State and 12 external contractor's access to MMIS was not removed timely upon termination. The APA noted users whose network access was removed so they could not access MMIS; however, their mainframe ID was not removed. DHHS relied on the external agencies to notify them of terminated users, they did not perform a regular review of external users to ensure user access is appropriate. DHHS did maintain a listing of MMIS external users; however, the list was not kept current.

- During a review of user access, we noted one employee of the Department of Education terminated and their access to the CNP system was not removed in a timely manner. For one of four terminations tested, we noted the Department of Education did not have documentation available to indicate network services staff was notified of the termination.

- One user's access to the network at the Department of Revenue had not been appropriately removed upon termination.

A similar comment was noted in prior IT audits.

When access to networks and applications is not terminated timely, it creates the opportunity for unauthorized access to State resources. When user statuses are not updated within an application to reflect their true status, application owners are unable to obtain an accurate listing of users.

> 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 LANs should be established and followed. Terminated users' access should be removed immediately. The creation, modification, and removal of users' 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:

Department of Correctional Services' Response: In response to the prior review, the Department of Correctional Services developed and implemented a formalized process to timely remove access to the Kronos application. The process was fully implemented in March, 2011. Portions of the process were implemented as early as July, 2010. At the date of the current audit, the semi-annual review of user access called for in the formalized process had not been implemented. That access review was scheduled for April, 2011. The Department believes the new process, with the inclusion of a semi-annual review of user access, has resolved the issue.

Department of Education's Response: For users external to NDE, there can be only a single district administrator for each district in the NDE Portal. When the districts submit changes in the Superintendent's position, the Portal Administrator removes that person's access from all accounts in the Portal, including the GMS.

For users internal to NDE, the Human Resources department notifies the NDE Portal Administrator as each employee leaves employment. The Portal administrator removes all accounts established in the name of that employee.

In the CNP, the employee access was removed and documentation is maintained as noted above.

Department of Roads' Response: We are developing a new User Access Request Application that we believe will help solve this problem. To help alleviate the issue of the user filling out the form, we will do monthly reviews of reports on unused userids' and contact Divisions to see if they can be eliminated.

Nebraska Supreme Court's Response: The AOC (Administrative Office of the Courts) has changed internal processes to provide a timely notice to the JUSTICE staff when an employee leaves or is terminated. Going forward this should remedy this situation.

Department of Health and Human Services' Response: DHHS has established a policy and procedure for reviewing user access and a formalized process to remove access for both internal and external users. Supervisors, security administrators and designated staff from contracted external partners have received the policy and procedures in writing and have had formal training. These policies have been shared with the State Auditor's office. The internal process involves completion of PAWS (Personnel Actions Workflow System) automated forms; the external process involves completion of automated forms by the contracted company and notification to the DHHS designated staff, who in turn notify the DHHS Help Desk. As noted by the audit – the process is impacted by the individuals responsible for completing the forms.

Department of Revenue's Response: The Department of Revenue agrees with the finding. The Department does follow a formalized process to remove access to both applications and network resources when users are terminated. However, there was a shortcoming in the procedure that resulted in the failure to remove access for certain terminated temporary employees. That shortcoming in the procedure has been corrected.

The Department will also implement two new periodic review processes to ensure the validity of user access:

1) *An annual review process for all active network accounts will be done by sectional management*
2) *Accounts that have been inactive for a period of four weeks will be reviewed.*

5. 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."

- 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.

- The APA noted 47 generic IDs were shared among users to gain access to the JUSTICE system.

- Three network IDs at the Department of Revenue did not appear appropriate as they were shared IDs and were not being used on a regular basis.

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:

Nebraska Supreme Court's Response: The AOC is actively working with users of shared ID's to eliminate this issue.

Department of Revenue's Response: The Department agrees with the finding. The Department will conduct a review of all network accounts to ensure that no shared network IDs are used to access applications or network resources unless there is a clear business requirement or system limitation. Any usage of shared IDs will be approved by the Agency Information Security Officer and documented.

6. 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.

Department of Correctional Services Administrative Regulation 104.06 states, in part, "The best passwords do not spell anything and contain a mix of upper and lower case alpha, numeric, and special characters. Passwords are required to be eight characters in length and contain three of these characteristics. The system will notify you if you do not meet this requirement and prompt you to select a new password that meets this strength standard."

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

- DHHS and the Department of Correctional Services' Kronos application for consecutive characters and special characters.
- The Department of Education GMS Portal login used by school districts for change requirement.
- DMV windows, VTR, and MCS applications did not force users to meet several NITC password requirements, including length, complexity, and reuse of passwords.
- The Department of Labor BPS application for minimum length.

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.

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.

7. Timeout Function

NITC Standards and Guidelines, Information Security Policy 8-101, Section 5, Physical and Environmental Security states, in part, "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 desktops, 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."

The Department of Roads had not enabled the timeout facility in the Windows environment.

Without procedures to enforce a timeout facility, there is an increased risk for unauthorized use of systems going undetected.

> We recommend the Department of Roads implement a timeout facility in the Windows environment.

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:

Department of Roads' Response: We will be implementing a timeout period within the next month.

8. 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."

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.

- The Department of Education did not have formalized change management procedures in place to include documentation of the change request, testing, and management approval for the change to be promoted into the production environment for the DDS application.
- A formalized Windows patch management and network change management process had not been implemented at the State Treasurer's office.
- DMV did not have formalized change management procedures in place to include a change request, test documentation, and management approval for the change to be promoted into the production environment for the MCS, VTR, and TSI applications, or for VTR and TSI database changes. There was 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 application and system changes. Additionally, individual agencies responses are listed below:

Department of Education's Response: DDS has established a more formal process for change management and have advised the audit staff of this.

State Treasurer's office Response: The Treasurer's office has part of patch management and network change management process in place, with the application change request procedure. The IT staff does document when they are applying Windows updates and installing software on servers.

Department of Motor Vehicles' Response: The DMV will review its existing change management process to identify and implement improvements to the process where necessary.

9. 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.

- 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 set up. 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. The Department of Roads is currently working on an upgrade to RBS that will address this issue.

- There was no documented review of the JUSTICE database logged changes. The OCIO maintains the logs; however, there should be a separate review to ensure all changes are approved and necessary.

A similar comment was noted in prior IT audits.

Without monitoring security violation reports, unauthorized users could access sensitive financial data on the network and financial applications without being detected.

> We recommend a periodic review of critical security events for unauthorized access and inappropriate changes be conducted and documented. We also recommend performing a documented review of audit logs and violation reports.

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:

Nebraska Supreme Court's Response: The AOC is actively working with the OCIO Mid-Range group to develop a periodic review process.

10. Business Processes

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

- The Supreme Court did not reconcile the number of paid JUSTICE case searches to the number of searches on the JUSTICE application. The JUSTICE application currently does not count the number of searches made on the application.

- DMV did not reconcile the number of record searches billed 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 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 do not agree to the Nebraska rates.

A similar comment was noted in prior IT audits.

When a reconciliation of searches is not performed there is an increased risk the agencies are 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 Supreme Court and DMV implement procedures to reconcile search activity to funds received. We also recommend the Department of Administrative Services work with Oracle to add an additional table for the State exemptions for State tax levies.

OCIO's Response: Individual agencies responses are listed below:

Nebraska Supreme Court's Response: The AOC has other priorities at the present time. This particular application averages about 300 transactions per month and the AOC does not feel the low volume warrants the development of an automated reconciliation process. A manual reconciliation is performed each month for this application.

Department of Motor Vehicles' Response: DMV conducts a reasonableness review of the monthly Payment Statements provided by Nebraska Interactive. After a review of possible changes to the DMV computer systems we have determined that there is not an automated solution available, within our current system, to perform a full reconciliation without the addition of at least one FTE. Such a solution is not cost effective considering the fact that the DMV only receives approximately 9% of the total remittance. Further, the following requirements in the Nebraska Interactive contract with the Nebraska State Records Board provide assurances that the proper financial processes are in place to ensure full payment for services provided:

- *Nebraska Interactive is contractually responsible for collecting and remitting all electronic access fees to the State of Nebraska on the last business day of the month.*
- *Nebraska Interactive is required to provide to the State of Nebraska, on an annual basis, an audited financial statement that discloses any discrepancies in their charges, billings or financial records.*
- *All of Nebraska Interactive books, records and documents directly relating to work performed or monies received and paid under its contract with the Nebraska State Records Board shall be subject to inspection and or audit by the APA.*

Department of Administrative Services' Response: We did receive a table from Oracle for the State Exemption piece, but it is part of the baseline upgrade that will need to take place. We will reiterate the importance of this issue, to see if it can be incorporated outside of the complete upgrade.

11. 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) 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."

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

- While the Department of Labor did have a business continuity plan, it did not appear to be complete; and disaster recovery could not be easily accomplished solely using the plan. The Department of Labor is in the process of performing a security assessment and plans to use that information to complete and update the business continuity plan. In addition, it was noted that backup data for the Department of Labor's NEworks system was not being stored offsite. The Department of Labor believed the OCIO was backing up and storing the data offsite; however, NEworks data had not been included in the OCIO's scheduled backup and tape run.

- The Department of Revenue did not have a disaster recovery plan in place for their Oracle applications. In addition, only monthly backup tapes were retained and stored offsite for these applications.

- NPERS did not have a completed disaster recovery plan in place. A plan had been started, but there were key processes that had not been documented within the plan. Per NPERS staff, as of May 18, 2011, the plan was 85 percent complete.

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.

> We recommend State agencies develop complete formalized business continuity plans, which includes testing and maintaining backup tapes off-site, to ensure data retention is effective.

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:

Nebraska Supreme Court's Response: The AOC agrees with this issue.

Department of Labor's Response: In the fall of 2010, NDOL received funding to conduct a security assessment and update of our contingency plan. The outcome of this project will provide processes, policies, and procedures for annual security assessments and contingency plan updates and testing. Upon completion, a copy of the security assessment and contingency plan will be provided to OCIO and the APA.

Daily offsite backups of the NEWorks servers began April 15, 2011. The servers are backed up daily. Additionally, there is a full copy of the NEWorks database stored on another server.

Department of Revenue's Response: The Department agrees with the finding. The Department currently performs daily backups of the Oracle systems and we started moving backup tapes off-site.

Nebraska Public Employees Retirement Systems' Response: The NPERS Disaster Recovery Plan has been completed and was reported as complete in the June 20, NPERS Retirement Board meeting. Tapes are maintained in off-site locations.

12. 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.

- One of twelve CNP edit checks tested at the Department of Education did not function as expected. Department of Education staff agreed that the edit was not working and have begun working with the application's vendor to correct the issue.

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

- In addition, the DHHS NFOCUS application contained a critical 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 erroneous or fraudulent eligibility determinations and or claim payments.

> We recommend State agencies work to ensure critical 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:

Department of Education's Response: The edit check in question has been corrected.

Department of Health and Human Services' Response: Edit checks – HEA (the application supporting the Home Energy Assistance program) is currently being rewritten. It does have limitations which are under review in the redesign. HEA will become an additional program in NFOCUS – targeted for implementation in July 2012.

In the second issue, DHHS policy is able to explain why the edit can be overwritten. However, since the audit, an additional SCR 11236 has been identified for some application changes to that area. Target implementation 3/11/2012.

13. Application Support

Good business practices include backup plans for unexpected interruptions to ensure any system downtime is kept to a minimum.

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.

When only one person is trained to support an application, there is an increased risk services supported by the application may be disrupted for a prolonged period of time.

> We recommend DMV evaluate the risks associated with relying on one individual to provide application support. We also recommend DMV 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 ensure essential programs have the appropriate level of trained resources. Additionally, individual agencies responses are listed below:

Department of Motor Vehicles' Response: The DMV is keenly aware that its limited application support resources exposed the agency to risks in its three main applications – VTR, TSI, and MCS. The DMV is not in a position to train additional staff to support the system, because no such additional staff exists within the DMV. Support for additional application support staff will have to come from the legislative and budgeting processes.

14. Physical Security Access

The APA noted concerns regarding physical security access. Due to the sensitive nature of the information in this comment, a separate non-public letter has been issued to the Chief Information Officer.

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's IT Systems gained during our work to make comments and suggestions that we hope will be useful to you.

This letter is intended solely for the information and use of the OCIO, 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.

We appreciate and thank all of the agencies' employees for the courtesy and cooperation extended to us during our audit.

Sincerely,

Signed Original on File

Jennifer Person, CPA, CFE
Audit Manager

Pat Reding, CPA, CFE
Assistant Deputy Auditor