ATTESTATION REVIEW
OF THE
STATE OF NEBRASKA
INFORMATION TECHNOLOGY SYSTEMS

JULY 1, 2009 THROUGH JUNE 30, 2010

Issued on August 12, 2010

STATE OF NEBRASKA INFORMATION TECHNOLOGY SYSTEMS
ATTESTATION REVIEW

TABLE OF CONTENTS

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

Independent Accountant's Report

Citizens of the State of Nebraska:

We have reviewed the Information Technology (IT) Systems General Computer and Application Controls of the State of Nebraska (State) as described in the Background Section of this report, for the period July 1, 2009, through June 30, 2010. The Office of the Chief Information Officer (OCIO) and each State agencies' management is responsible for the IT Systems General Computer and Application Controls. We did not obtain a written assertion regarding such matters from management.

Our review was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States. A review is substantially less in scope than an examination, the objective of which is the expression of an opinion on the State's IT Systems General Computer and Application Controls. Accordingly, we do not express such an opinion.

Based on our review, nothing came to our attention that caused us to believe that the State's IT Systems General Computer and Application Controls are not presented, in all material respects, in conformity with the criteria set forth in the Criteria section.

In accordance with *Government Auditing Standards*, we are required to report findings of deficiencies in internal control, violations of provisions of contracts or grant agreements, and abuse that are material to the State's IT Systems General Computer and Application Controls and any fraud and illegal acts that are more than inconsequential that come to our attention during our review. We are also required to obtain the views of management on those matters. We did not perform our review for the purpose of expressing an opinion on the internal control over the State's IT Systems General Computer and Application Controls or on compliance and other matters; accordingly, we express no such opinions.

Our review disclosed no findings that are required to be reported under *Government Auditing Standards*. However, we noted certain other matters, and those findings, along with the views of management, are described below in the Summary of Results.

This report is intended solely for the information and use of the Citizens of the State of Nebraska, management of each State agency, others within the State, and the appropriate Federal and regulatory agencies. Although it should not be used by anyone other than these specified parties, this report is a matter of public record and its distribution is not limited.

Signed Original on File

Mike Foley
Auditor of Public Accounts

Jennifer Person, CFE
Audit Manager

August 12, 2010

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 (Reissue 2008, as amended by 2010 Neb. Laws, LB 1071, § 41). 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 (Reissue 2008) 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 NITC are defined by Neb. Rev. Stat. § 86-516 (Reissue 2008, as amended by 2010 Neb. Laws, LB 1071, § 40) 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 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.

The OCIO and 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), formerly the Nebraska Information System (NIS)*** – 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 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.

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.

Nebraska Public Employees Retirement System (NPERS):

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

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.

Department of Revenue:

- ***Tax Processing Applications*** – The Department of Revenue utilizes multiple tax processing applications. These tax applications include, but are not limited to the processing of: sales tax, corporate and individual income tax, fiduciary tax, motor fuels tax, motorboat tax and fees, cigarette tax, waste reduction and recycling fees, tire fees, litter fees, lodging tax, and drug tax. Additional applications track and process charitable gaming licenses, Homestead Exemption for property tax, fertilizer fee systems, and the partnership system. Tax refund payments interface with EnterpriseOne.

- ***NebFile*** – The NebFile application allows Nebraska resident taxpayers to file their State income tax return free over the Internet. NebFile is not tax preparation software, but will do simple calculations and table look-ups for the taxpayer. The NebFile system allows individuals to file a short form, Form 1040NS, or a long form, 1040N, with some limitations.

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.

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.

Criteria

The criteria used in this attestation review were the Nebraska Information Technology Commission Standards and Guidelines, good internal controls, and sound business practices.

Summary of Procedures

Pursuant to Neb. Rev. Stat. § 84-304 (Reissue 2008), the Auditor of Public Accounts (APA) conducted an attestation review of the State's IT Systems General Computer and Application Controls for the period July 1, 2009, through June 30, 2010, in accordance with standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States. The APA's attestation review consisted of the following procedures:

- Performed general and/or application control testing of the following applications:
  - EnterpriseOne
  - Kronos
  - Medicaid Management Information System (MMIS)
  - Nebraska Family Online Client User System (NFOCUS)
  - Benefit Payment System (BPS)
  - Children Have a Right to Support (CHARTS)
  - Tax Management System (TMS)
  - Project Finance System (PFS)
  - Roads Payment System (RPS)
  - Roads Billing System (RBS)
  - General Ledger System (GLS)
  - JUSTICE
- Performed general control testing of the State's mainframe housed at the OCIO.
- Obtained a general understanding of the flow of information with Nebraska Interactive regarding Nebraska.gov and other contracted web hosting.
- Followed up and assessed the status of prior IT findings.
- An exit conference was held on July 21, 2010, to discuss the results of this attestation review. Those in attendance from the OCIO were:

  Brenda Decker, Chief Information Officer
  Brad Weakly, State Security Officer

Summary of Results

The summary of our attestation review noted the following findings and recommendations:

1. Developer Access to Production Environment

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 requires access to information resources to be restricted based upon job responsibilities to help enforce proper segregation of duties and reduce the risk of unauthorized system access. Programmers should be expressly prohibited from directly accessing data and production software.

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

- NDE had Quest application developers, two DDS application developers, two Social Security Administration DDS contracted developers, and two GMS application developers with access to his or her respective production environments.

- The Department of Labour had two developers utilizing a shared ID with super user access to BPS. Their actions were logged and reviewed; however, the review was not documented.

A similar comment has been 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 that has been processed.

> 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 work with the agencies identified to resolve the internal control issues identified and ensure the production environments are protected from unauthorized changes. Additionally, the Department of Labor (Labor) is currently reviewing BPS logs and has implemented a process to document the review. Labor has also changed the reporting structure in IT to create separation of duties and management between developers and DBAs. A process has been implemented for management review and approval of all BPS changes prior to moving into production.

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."

NITC Standards and Guidelines, Information Security Policy 8-101, Section 9, System Development and Maintenance states, in part, "Separation of the development, test and production environments is required, either on physically separate machines or separated by access controlled domains or directories."

Good internal control requires logical access to systems to be 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 access that is not appropriate, significant information resources may be modified inappropriately, disclosed without authorization, and/or unavailable when needed.

- We noted 7 of 128 active mainframe user IDs with special attributes that did not require the access based on their job responsibilities. One of those IDs was assigned to a user who retired from the State in April 2004. Five users were accountants or program managers whose agencies had a 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.

- The activation code allowing NDE employees staff level access to the GMS application was the same for each user and was not changed on a periodic basis. Policies and procedures had not been established to document NDE staff level user provisioning for the GMS application.

- There was one BPS user ID that did not require the elevated access; however, it did not appear the ID had been used based on the time stamp.

- There was one JUSTICE programmer ID that was not required because the individual changed job responsibilities. The access to JUSTICE has been subsequently removed.

A similar comment has been 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 the 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 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, the Department of Labor has deleted the user ID identified above. In the BPS application the authorized role 'CC Supervisor' is being changed, so the role cannot modify a user's access. A new authorized role 'modify user' will become a separate authorized role and be restricted to management. Labor is in the beginning phase of developing an automated workflow process through Enterprise Content Management to approve and provide access to systems by job description/duties. The workflow is triggered by a personnel action (new, changed or terminated) and approved by the application owner. The workflow will include periodic review of the list of users by application owners to verify appropriate access 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 requires those individuals who develop system changes to not have access to production datasets. Logical security tools and techniques are 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 the production datasets for the CHARTS application. In addition, there was one shared on call user ID with alter access to CHARTS production datasets.

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

- Twelve developers had alter access to the production datasets of the NFOCUS application.

- Three developers had alter access to the production datasets of the HEA application.

A similar comment has been 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 work with the agencies identified to evaluate the potential options to restrict application developer's access to the production environment and create the appropriate monitoring controls.

4. New and 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."

Good internal control requires new user access be properly approved and terminated users access be removed timely.

- For 18 of 25 terminated EnterpriseOne users tested, the access was not removed in a timely manner. Ten of the individuals noted had self service inquiry access while eight individuals had functional access within EnterpriseOne. Agencies were not communicating with the Department of Administrative Services to ensure access was removed on a timely basis.

- 47 Department of Correctional Services Kronos users had either terminated or changed job responsibilities; however, their access had not been removed. In addition, a number of terminated individuals access had been removed from Kronos; however, they still had an active AS/400 ID.

- There was no process to ensure 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.

- The Department of Labor reused their Resource Access Control Facility (RACF) IDs. Due to this, the APA was unable to determine whether the user had their access removed in a timely manner for all five terminated Department of Labor RACF users tested. RACF is used to control user access to the Department of Labor's mainframe applications. The APA also noted seven BPS application users had either terminated or transferred to another agency; however, their access had not been removed. One of the seven individuals noted terminated in January 2007.

- The Department of Roads did not remove terminated employees' access to the network timely for six of ten employees tested. One of six individuals had remote access for 52 days after their termination date.

- 24 Supreme Court JUSTICE users had terminated; however, their access had not been removed. One of the individuals noted terminated in November 2005. A number of terminated individuals access had been removed from JUSTICE; however, they still had an active AS/400 ID.

- For five of twenty-five terminated DHHS users tested, access was not removed from the network in a timely manner. Two of the terminated users also had access to NFOCUS. The access was removed between seven and thirteen days after their termination date.

- The APA could not verify the ACTS accounts were disabled in a timely manner for three temporary employees tested. Documentation was not maintained to support when the employee terminated. The APA also noted three additional DHHS employees whose access to ACTS was not removed timely and there was no documented review of user access to the application.

- Two CONNECT super users did not require access as they had moved divisions within DHHS in 2007. These users were noted in our prior report but were not removed. Access to the CONNECT application was controlled by the ARGUS application which did not store dates of when a user's access was created, modified and/or removed. There was also no documented review of users with the ability to assign roles in Argus.

- For one of ten new hires tested, access to BPS was not properly approved by the Department of Labor's management.

- For one of twenty-five new mainframe access IDs tested, the OCIO did not have an access ticket on file. In addition, three IDs were not assigned to an individual, but were still given out to the Department of Correctional Services and DHHS.

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

We recommend application owners review user access on a periodic basis to ensure access is appropriate. Additionally, a formalized process to grant and remove access to applications 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 work with the agencies identified to establish a review schedule of all users of applications and formalize a process to grant and remove access to these applications.

The EnterpriseOne team responds to termination requests and access is removed by the EnterpriseOne team in a timely manner. As the State moves to a more tightly integrated solution for access, EnterpriseOne, as well as other systems, will not have the need to rely so heavily on the agencies reporting or lack of reporting this information to their agency.

Additionally, the Department of Corrections has indicated that they will improve management of user access to the Kronos system by convening a workgroup of HR, Accounting and IT staff, tasked with identifying, documenting, and implementing a standard process for 1) ensuring timely granting and removal of access to the Kronos system, 2) for maintaining documentation of access, and 3) for periodic review of access granted. The new process will be in place by September 30, 2010.

The Department of Labor (Labor) has eliminated the reuse of RACF IDs. Labor is in the beginning phase of development of a new workflow process as described in the response to point 2 to include proper management approval. In the meantime, Labor is reviewing their manual process with more rigor to ensure management has given the proper approval. Labor's Internal Security unit is setting up a check and balance review of all access and terminations. The access/termination request is validated by a different staff person than the staff person actually processing/terminating the access to verify the required action was completed. The Department of Labor is currently using a manual process for granting and removing access to systems and applications. That process has recently been modified to include notifications from HR to managers/supervisors to request they fill out the appropriate forms for system/applications access or removal. The notifications are triggered by a personnel action (new, changed, terminated). Labor is in the beginning phase of creating an automatic workflow process through Enterprise Content Management for access approvals, configurations, and terminations to ensure proper documentation of a user's access and immediate removal of terminated users access.

The Department of Roads is working from an old Lotus Notes application that handled new user requests/resignations. The Department of Roads is in the process of rewriting the application and believes this will improve the process.

The Administrative Office of the Courts JUSTICE team has changed internal practices so their Business Analysts are notified by their HR staff when a person retires, is terminated or leaves the branch. This will allow for the prompt cancellation of IDs and notice to the OCIO Mid-Range staff to cancel IDs in the AS-400 as well.

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."

Good internal control requires users to maintain unique IDs to access systems.

- Two system IDs for the EnterpriseOne application that administer and support its platform and application were shared among several users. An individual reviewed the logs of individuals using the shared IDs; however, the log did not identify who used the ID.

- The Department of Labor maintained four generic IDs used for temporary staff to gain access to TMS.

- DHHS maintained three IDs with administrative privileges to the WIC application that were shared amongst certain staff members. All changes were logged within the system; however, there was no documented review of the changes made with these IDs.

- The State Treasurer's office maintained one shared ID with access to forcibly balance reports in Wagers and management did not perform a documented review of the these reports.

- The APA noted 47 generic IDs that were shared among users to gain access to JUSTICE. One of the IDs is shared by the Supreme Court's technical analysts to access production servers in all of the counties.

A similar comment has been 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 to ensure individuals have a unique ID to make users accountable for transactions on computer systems.

OCIO's Response: The Office of the CIO will work with the agencies identified to eliminate all shared IDs for accurate accountability. The EnterpriseOne technical team will implement new procedures to monitor and follow-up with those individuals utilizing the QSRV and QSECOFR IDs in order to determine the need for signing on to the AS400 with these IDs. The Department of Labor has eliminated the reuse of generic IDs for temporary staff, as well as eliminating the reuse of LABZ IDs and temporary IDs. Additionally, the Administrative Office of the Courts JUSTICE team continues to work to reduce the number of shared IDs in the system. As for the Technical Analysts having a shared password this is due to the 94 AS-400s located within the state and to require individual access on all AS-400s would be a burden and reduce productivity and delay response to correcting critical problems.

6. Password Complexity

NITC Standards and Guidelines, Password Standard 8-301, Section 2.1, Password Construction, requires the following 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 requires passwords be changed periodically and the complexity of the length or types of passwords be maintained at all times.

Password policies did not meet the minimum requirements of the NITC standard above as follows:

- EnterpriseOne for length, consecutive characters, and special characters.

- The Department of Correctional Services' Kronos application for length, consecutive characters, and special characters.

- The DHHS ACTS application for change requirement and repeat of passwords used during the previous 365 days.

- The DHHS CNP application for change requirement.

- The NDE GMS Portal login used by school districts for change requirement.

A similar comment has been 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 compliance with NITC requirements.

OCIO's Response: The Office of the CIO will work with the agencies identified to ensure NITC compliance and/or exceptions will be documented through the NITC process. The EnterpriseOne technical team will implement new password complexity for the system. The EnterpriseOne system now allows us to implement more complex password rules. When the OCIO implements a Single Sign-On solution for the State of Nebraska, EnterpriseOne will be participating and the password complexity will be driven by the OCIO. Additionally, the Department of Correctional Services will work with DHHS and OCIO, through the bi-monthly Kronos Change Management meetings, to review current password policy against NITC standards, to amend password security configuration to comply with NITC standards or if compliance is not feasible to request appropriate NITC waiver of standard(s). Review of password policy took place in the July, 2010 Kronos Change Management agenda. The Change Management team agreed to request a temporary waiver from NITC, pending completion of the currently scheduled Kronos version upgrade, with the goal of implementing password configuration changes as part of the version upgrade. The Kronos group is currently developing an NITC waiver request.

7. 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 requires a formal methodology to be in place 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.

- NDE did not have formalized change management procedures in place to include a request, test documentation, and management approval for the change to be promoted into the production environment for the DDS application. In addition, there was no documentation on file for one of three changes tested made to the CNP application.

- Two of twenty-five BPS changes, tested by the APA, were developed, tested, and moved into production by the same individual.

- During testing of ten changes made to the Department of Roads IT environment we noted one General Ledger System change and one system software change was not approved. Also, Windows updates were not tested before migration to production.

- Changes to the Wagers application were tested prior to moving into production; however, the testing was not documented. In addition, a formalized Windows patch management and network change management process had not been implemented at the State Treasurer's office.

A similar comment has been 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 decreased financial data reliability.

> 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 work with the agencies identified to establish standardized change management processes of application and system changes. Additionally, the Department of Roads (Roads) does have a standard change management process in place. Road's management will once again stress the importance of testing and making sure the changes are approved. The Department of Labor is in the process of redesigning the current change management system to manage production support changes (batch failures) separate from other changes (i.e. defects), which requires management approval before moving into production. Labor will continue to work to document change requests, approvals, and testing procedures, requiring management approval of all changes into production.

8. 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 requires computer systems to be adequately monitored to verify they are operating according to management's expectations.

- The Department of Roads' network logs were enabled but were not reviewed. 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 State Treasurer's Wagers application audit logs were maintained for deletions and gaps in transactions; however, no one reviewed the logs for appropriateness.

- Monthly network audit logs for the Department of Revenue were maintained but review of the logs was not documented.

A similar comment has been 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 monthly review of critical security events for unauthorized access and inappropriate changes be conducted and documented. We also recommend a documented review of audit logs and violation reports.

OCIO's Response: The Office of the CIO will work with the agencies identified to establish a documented, scheduled review process of security events. Additionally, the Department of Revenue (Revenue) has set up a process where the Network administrator will review the monthly audit reports. The reports will be saved to a directory on Revenue's network. The network administrator will use a spreadsheet in that directory to sign off on the review. In addition, an email will be sent to the IT Services Manager verifying that the review was done each month. Roads is in the process of installing and configuring Microsoft's Systems Center Operation Manager to review the log files. For the Roads RBS application the Director has recently approved a project to modify the application in order to eliminate the problem.

9. Business Processes

Good internal control requires 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. When a reconciliation of searches is not performed there is an increased risk the agency is not receiving all funds due to them.

- The Department of Administrative Services did not use the correct tables when calculating the exemption for the State tax levy within EnterpriseOne for State employee garnishments. They had been using the Federal exemption amounts which do not agree to the Nebraska rates. When the correct table for State tax levies is not used, the employee's pay is calculated incorrectly.

We recommend the Supreme Court implement procedures to reconcile the search activity on JUSTICE to the 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: The Administrative Office of the Courts (AOC) feels this would be financially costly with little return to show for the effort to program this functionality into JUSTICE. This application also allows for state and local government to search for free. At this time the AOC does not intend to implement this recommendation as the risk is very low that searches are not being reported or are not accurate.

APA Response: Procedures should be implemented to ensure all funds due the Supreme Court are received in relation to paid case searches.

10. 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."

Good internal controls require a formalized, tested plan of procedures and organization designed to safeguard assets and minimize the risk data is lost.

- NDE did not have adequate procedures to ensure essential business processes and information systems could be recovered timely. NDE had not tested the GMS backup tapes to ensure their completeness and had not developed a formalized business continuity plan.

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

- NPERS did not have a completed disaster recovery plan in place. A plan has been started, but there were key processes that had not been documented within the plan.

A similar comment has been noted in prior IT audits.

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

We recommend State agencies develop complete formalized business continuity plans and backup tapes be tested and maintained off-site to ensure data retention is effective.

OCIO's Response: The Office of the CIO will work with the agencies identified to establish formalized business continuity plans with effective data retention testing and storage. Additionally, the Nebraska Public Employees Retirement Systems (NPERS) notes that much work has taken place on their plan since January of 2010. The NPERS plan has basically gone from an "outline" form with no documented procedures to approximately 65% completion. Some sections of the plan are now 100% complete. The initial work on the NPERS DR Plan has been reviewed by the OCIO and a meeting was held to gain insight and direction on the plan. The target date for completion of the plan is November 2010. That date was given to the Retirement Board in a public meeting held in May, 2010. NPERS is storing backup tapes offsite with the OCIO on an ongoing basis and has established a secondary backup tape operation with Superior Data Storage that has been in place since December of 2009. NPERS User Acceptance Testing (UAT) servers have been relocated to the OCIO server room to serve as our Disaster Recovery platform in the event that a disaster should occur.

11. 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.

Overall Conclusion

We noted several instances where State agencies did not appear to be in compliance with NITC Standards and Guidelines. These included a lack of segregation of duties, excessive access, a lack of periodic reviews of users, lack of documentation to support change management processes, and inadequate password parameters. A number of these issues were noted in our previous IT audits.

The APA staff members involved in this attestation review were:

Jennifer Person, CFE, Audit Manager
Craig Kubicek, CPA, CFE, Auditor-In-Charge
Tyler Niday, CPA, CISA, Auditor-In-Charge
Philip Olsen, CPA, CISA, Auditor-In-Charge
Marta Schrock, Auditor-In-Charge
Zachary Wells, CPA, Auditor-In-Charge
Acacia Crist, CFE, ACDA, Auditor II

If you have any questions regarding the above information, please contact our office.