ATTESTATION REVIEW
OF THE
STATE OF NEBRASKA
INFORMATION TECHNOLOGY SYSTEMS

JULY 1, 2008 THROUGH JUNE 30, 2009

Issued on November 18, 2009

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 the report, for the period July 1, 2008, through June 30, 2009. The Office of the Chief Information Officer (OCIO) and each State agency's 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; however, 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

November 18, 2009

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). 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 enterprise projects.

Neb. Rev. Stat. § 86-515 (2008) created the Nebraska Information Technology Commission 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 (Reissue 2008) 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 Nebraska Information Technology Commission (NITC) to ensure cost-effective and efficient use of State resources and investments in information technology. The OCIO assists the 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:

- ***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 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 NIS.

- ***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 NIS.

- ***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 NIS.

- ***Home Energy Assistance (HEA)*** – This application supports the Federally funded Low Income Energy Assistance Program (LIEAP). 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 NIS.

- ***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 user 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 in the system is utilized for numerous activities such as; tracking, authorizations, notification, data, quality assurance, and payment to contracted services coordination agencies for services coordination. Some CONNECT payments interface with NIS.

- ***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 NIS 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 NIS.

- ***Disability Determination System (DDS)*** **–** The 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 NIS.

- ***Child Nutrition Program (CNP)*** **–** The 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 NIS 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):

- ***Pension Information of Nebraska for Efficient and Effective Retirement (PIONEER)*** **–** The PIONEER application processes contributions from members and employers and prepares information for NIS to print member benefit payments.

- ***Nebraska Public Retirement Information System (NPRIS)*** **–** This application replaced the PIONEER application's processes in March 2009. It processes contributions from members and employers and prepares information for NIS to print member benefit payments.

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 NIS.

- ***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.

- ***Maintenance Management System (MMS)* –** MMS manages labor, equipment, materials, maintenance contracts, and indirect costs for routine highway maintenance.

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

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

State Treasurer's office:

- ***KidCare*** – The KidCare application supports child support payment processing, including receipt and disbursement 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 Nebraska Information Technology Commission (NITC) 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, 2008, through June 30, 2009, 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:

1. Performed general and/or application control testing of the following applications:
   a. Child Nutrition Program
   b. Coordinating Options in Nebraska's Network Through Effective Communication and Technology
   c. Medicaid Drug Rebate
   d. Medicaid Management Information System
   e. Nebraska Family Online Client User System
   f. Benefit Payment System
   g. Tax Management System
   h. Nebraska Public Retirement Information System
2. Followed up and assessed the status of prior IT findings.

3. Obtained an understanding of the Department of Motor Vehicles' driver licensing system implementation issue that occurred on July 19, 2009. See **Exhibit A**.
4. Obtained an understanding of the Department of Health and Human Services contract for replacement of MMIS and termination of the contract. See **Exhibit B**.

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 generally be limited to accessing only the information specifically required to complete their assigned system development projects. They should be expressly prohibited from directly accessing production software and data information. Computer operators normally should be permitted to run production jobs; however, they should be restricted from accessing the development environment. Access to production program libraries and data information should be logged and periodically reviewed for appropriateness.

- Two application developers at the State Treasurer's office had administrator access to the Windows environment and to the KidCare application's database. The application developers also had administrative access to the KidCare application. The State Treasurer's office plans to look into ways to monitor changes made by developers.

- Department of Revenue application developers had the ability to develop and promote changes to production in the GPS, Homestead Exemption, Motor Fuels, Charitable Gaming, and Motorboat applications. Procedures have been developed to remediate this issue. The Department of Revenue was still working on the implementation of the procedures, which included training staff, reassigning duties, and assigning access rights to applications at the end of fiscal year 2009.

- Three Identifiers (IDs) used by contracted developers and two NDE application developers had a level of access to certain GMS database(s) that allowed them to change the configuration of production data or grant access to databases. Developers and contractors do not require this access to perform their job functions and should not have this capability.

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

A similar comment has been noted in prior IT audits.

Application developers with access to the database and the production environment have the ability to circumvent the standard change control process and implement modifications that may not be consistent with management's intentions. This creates a risk that unintended changes may occur to data that has been processed.

> Depending on the size of the information technology department, developers may need access to the production processing environment. In order to mitigate the risk of moving unintended changes into production, compensating controls should be established. We recommend developers be required to obtain approval prior to moving changes into production. In addition, a compensating control such as review of audit logs or automatic notification should be established to identify all changes made to the production environment.

OCIO's Response: See response after Finding 11.

2. <u>Access Commensurate with Job Responsibilities</u>

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 controls require logical access to systems 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. Unauthorized modifications to job scheduling software may result in incomplete or inaccurate processing. If such access is not implemented and configured properly, business cycle controls may be ineffective. When users are granted access that is not commensurate with his or her job responsibilities, significant information resources may be modified inappropriately, disclosed without authorization, and/or unavailable when needed.

- 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 NDE CNP Administrator ID which was generic in nature and was not required as a system ID. This ID has been subsequently removed.

- The State Treasurer's Wagers Unclaimed Property Application allowed users to forcefully balance a report that is not in balance. Three individuals had access to the tool to forcefully balance a report. The State Treasurer's office is in the process of requesting logs that will be reviewed, including when reports are forcibly balanced.

A similar comment has been noted in prior IT audits.

When an individual has access not required by his or her job duties, there is an increased risk for the loss of State funds due to error or fraud. There is also a risk that unauthorized transactions or changes could occur. 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 their users and verify access levels are accurate. This should be done on a periodic basis to ensure access to the application is commensurate with employees' job responsibilities.

OCIO's Response: See response after Finding 11.

3. <u>Dataset Access</u>

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 individuals who develop changes for systems to not have access to production datasets. Typically, entities restrict access to information resources (e.g., programs, data, networks) to enforce desired segregation of duties, facilitate on-line approvals, and help achieve business cycle control objectives. 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.

- Four OCIO developers had access to production datasets for the Corporate Income Tax and Individual Income Tax mainframe applications. The Department of Revenue and the OCIO are working to review weekly access reports of developers to these production datasets.

- Two developers had alter access to the production datasets for the DHHS CHARTS application. In addition, there was one shared on call user ID with alter access to CHARTS production datasets. The activity performed using this ID was logged; however, no periodic documented review of the log was performed.

- Two developers had alter access to the production datasets of the DHHS MMIS application. In addition, one user ID with alter access to MMIS production datasets did not require this access to complete their job responsibilities.

- 45 developers had alter access to the production datasets of the DHHS NFOCUS application. In addition, there were 56 shared "test" user ID's which should have never been granted alter access to the NFOCUS production datasets. There were also 38 user IDs which did not require alter access to the NFOCUS production datasets to complete their job responsibilities.

- Two developers had alter access to the production datasets of the DHHS HEA application. In addition, two user IDs did not require access to the HEA production datasets to complete their job responsibilities.

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 production are appropriately approved and tested.

OCIO's Response: See response after Finding 11.

4. <u>New and Terminated User Access</u>

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 upon termination.

- There was not an adequate review of Resource Access Control Facility (RACF) users periodically performed or initiated by the OCIO to identify terminated users and ensure access was reasonable. The last review was completed in July 2008. The APA noted an increase of approximately 200 inactive IDs compared to the number of inactive IDs for fiscal year 2008. Over 1,600 IDs were inactive and revoked as of August 2009. RACF is a tool used by the OCIO to control user access to the states various mainframe applications.

- We noted a NIS server user profile established for a consultant, to assist with the November 2008 employee open enrollment process was not disabled once open enrollment was completed. This profile has subsequently been removed.
- 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 DHHS ACTS application does not store dates of when a user's access was created and/or modified. For one of two terminated users tested, we were unable to determine whether the user had their ACTS access removed in a timely manner. In addition, management did not document the review of user access.
- Access to the DHHS 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. For one of three new users tested, no documentation was on file to support the access given.
- There was no documented review of user access for the DHHS CONNECT application.
    - Two roles were no longer being used; however, one role was assigned to four users and the other role was assigned to one user.
    - For two of twenty-two users assigned the super user role, the access was no longer needed to complete necessary job functions. The employees changed divisions within DHHS and no longer required super user access. The users switched divisions in August 2007 and November 2007.
- For the DHHS CONNECT application, there was no documented review of user's with ability to assign roles for the application. One of eight users with the ability to assign roles had not utilized this ability in their current position and no longer needed the access.

A similar comment has been noted in prior IT audits.

The identification and authentication of users validate the individuals who use computer systems. Inadequate approval of access or a lapse in removing access may lead to financial loss, operational damage through unintentional access, or deliberate unauthorized access. 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 user's access should be documented and include a date stamp.

OCIO's Response: See response after Finding 11.

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 profiles for the NIS server were shared among several users.
- DHHS utilized two shared user IDs with administrative privileges for the WIC application. The actions of the two IDs were logged within the system; however, no one reviewed the logs. In addition, there was one shared user ID for temporary workers with access to the WIC application.

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: See response after Finding 11.

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 to be changed periodically and complexity of the length or types of passwords be maintained at all times.

We noted the following relating to passwords:

- Passwords for the NDE GMS Portal login could be utilized for an unlimited amount of time with no change requirement.

- The password policy for NDE's CNP application did not meet NITC minimum guidelines for expiration, special characters, and password history.

- DHHS did not have password parameters enabled for the ACTS application. In addition, super users had access to a table within the ACTS application that was not encrypted.

- The DHHS CONNECT application was accessed through the State's portal at my.ne.gov. There was no password parameter preventing the user from repeating any of the passwords used during the previous 365 days.

A similar comment has been noted in prior IT audits.

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

> We recommend password complexity requirements be implemented. In addition, sensitive tables should be encrypted within the application.

OCIO's Response: See response after Finding 11.

7. <u>Physical Security</u>

Good internal control requires only appropriate individuals have access to high level security areas such as a server room.

When reviewing access to the DHHS computer server room, we noted 207 active badges could access the room. The APA received a list of the individuals who actually accessed the server room between the dates of February 28, 2009, and August 27, 2009; this list showed 53 of the 207 badges were actually used to enter the room. Three of the 53 badges actually used belonged to cleaning staff and a total of 55 active badges were assigned to cleaning staff. Most of the remaining badges that were not used belonged to DAS-Maintenance and State Patrol Security Staff. It appeared that access to critical systems was given to many individuals who did not need the access. A log was maintained of those who actually accessed the room; however, this log was not reviewed.

Physical access to information resources makes it possible for the user to view, use, damage, or misappropriate these resources. Potential consequences of weakness in physical security could be accidental or intentional violations including damage to equipment and property, theft of equipment, property, or documents, copying or viewing sensitive information, and abuse of data resources.

> We recommend DHHS review the list of individuals with access to the server room to determine whether all individuals need the access. DHHS should work with DAS and the State Patrol to ensure all individuals need access to the server room. We further recommend DHHS perform a documented periodic review of the access log.

OCIO's Response: See response after Finding 11.

8. <u>Standardized Change Management Process</u>

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 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.

- The Department of Roads had developed procedures for a standard and consistent change control process for database and application modifications, but had not implemented the procedures by the end of fiscal year 2009.

- Both of the changes made to the DHHS CONNECT application during fiscal year 2009 did not have documentation to support the change had been tested prior to being promoted to production.

- Both changes to the DHHS MDR application tested by the APA did not have adequate documentation to support the change was approved by management, tested, and approved for promotion to production.

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, application 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 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: See response after Finding 11.

9. <u>System Monitoring</u>

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 be adequately monitored to verify they are operating according to management's expectations.

- The State Treasurer's Wagers application had audit logs showing activity of deleted transactions and breaks in the sequential numbering of transactions; however these logs were not reviewed for appropriateness.
- The Department of Roads' RBS application did not have the capability to record which user completed each part of the accounts receivable and receipting process for subsequent review.
- The DHHS ACTS application did not have adequate security tools in place. The application did not log security events, super user access, or access to sensitive data. The application would record only the most recent activity and would not log a complete history of user activity.

A similar comment has been noted in prior IT audits.

Without monitoring and reviewing data logs to ensure processing occurred successfully, there is an increased risk unauthorized, incomplete, or inaccurate processing will go undetected. 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. We also recommend the review of audit logs and violation reports.

OCIO's Response: See response after Finding 11.

10. Reconciliation and Payment Process

Good internal control requires an adequate segregation of duties between the individual who processes payments and the individual who reconciles the payments. Good internal control also requires procedures to ensure payments are made only once.

The individual who reviews the automated reconciliation between GMS and NIS for NDE could also process payments in GMS. In addition, the payment batch file created in GMS could be resubmitted. The duplicate batch should be caught during the interface reconciliation, but since the individual who does the reconciliation can also create payments there is a risk of the duplicate batch going undetected.

This was noted in prior IT audits.

> We recommend NDE ensure there is an adequate segregation of duties within the GMS payment process. The individual responsible for the reconciliation of payments should not have access to process payments.

OCIO's Response: See response after Finding 11.

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."

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. Additionally, the backup tapes for the DDS application were stored at another building across the street, which would be ineffective in the event of a major disaster.

- NPERS servers were not set up to notify IT staff in the case they were to lose power during non-work hours. This would not allow NPERS staff time to shut the systems down properly when not present at NPERS offices.

A similar comment has been noted in prior IT audits.

When tested comprehensive continuity plans are not in place and tapes are not tested, there is an increased risk for the loss of data.

> We recommend backups are tested and taken offsite to ensure data retention is effective and also to develop a tested comprehensive business continuity plan.

OCIO's Response: The Office of the CIO agrees with the recommendations and will work with the agencies identified to assist in establishing a process to implement the change management procedures outlined. Additionally, the Office of the CIO will refer several of the recommendations to the Security Architecture Work Group of the Technical Panel of the NITC. It is our intent to recommend that the Work Group consider the inclusion of language addressing some of these best practices in the NITC policies to address these issues with all State agencies. Finally, for those items identified that already are covered in NITC standards and guidelines, the Office of the CIO will work with the agencies identified to assure compliance.

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 a periodic review of users, lack of documentation to support change management processes, and inadequate passwords.

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, Auditor-In-Charge
Philip Olsen, CPA, CISA, Auditor-In-Charge
Marta Schrock, Auditor-In-Charge
Zach Wells, CPA, Auditor-In-Charge
Acacia Crist, CFE, ACDA, Auditor II
Mary Avery, Special Audits and Finance Manager

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

Exhibit A

STATE OF NEBRASKA INFORMATION TECHNOLOGY SYSTEMS

DEPARTMENT OF MOTOR VEHICLES DRIVER LICENSING SYSTEM IMPLEMENTATION ISSUE

The Nebraska Department of Motor Vehicles (Department) was implementing a new version of the driver licensing system when a power blip caused the implementation to be interrupted. Through inquiry of the Department and the Office of the Chief Information Officer (OCIO) the following is a summary of the issue and resulting resolution process.

The Department's driver licensing system resides on the mainframe and the counties utilize the AS/400 to run the licensing program. In order to implement the new licensing system, the mainframe, the AS/400, and the new system had to be linked together for the implementation to process to completion. The Department's goal was to have the new system implemented and fully operational for business on Monday, July 20, 2009, for the 13 county offices that operate 5 days a week.

Ten install teams were involved in the implementation process throughout the weekend. Those ten teams were deployed to Department/County locations around the State; their primary mission was to remove old hardware and install new hardware, as well as test each location to ensure the new system was properly installed in each of the 13 5-day a week locations. The existing licensing system was brought down after the close of business on Friday July 17, 2009; old hardware removed and new hardware was installed and the installation of the new version of the driver licensing system began on Saturday, July 18, 2009.

On Sunday, July 19, 2009, two brief power blips occurred sometime between 6:50 p.m. and 7:40 p.m. per the Department's communication with the Lincoln Electric System. The two blips caused an interruption between the three systems during the implementation process. Once the process was interrupted the implementation was at a standstill until the install team and the new licensing system vendor could diagnose what affect this blip had on each system and then address at what point the implementation could be resumed. Once the problem was diagnosed and it was determined there was no hardware failure or data loss, the install process resumed.

The APA discussed this issue with the OCIO which noted they did not register any outage on their systems. Since this was just a blip in power, the systems would not have come down and it would not have registered as an outage to the OCIO.

The driver licensing stations were closed for business until the implementation was complete because once the implementation started there was no going back to the old system – old hardware had been removed and the old system was off-line. The technology prohibited the Department from running the old and new systems simultaneously.

At about 11:00 p.m. Sunday, July 19, 2009, it was determined the licensing system would not be up and running for the 13 county offices for Monday, July 20, 2009, the anticipated go live date. The Driver Licensing staff were in a paid stand-by status for about 1 ½ days to ensure that staff would be present and the offices could open as soon as the new system was operating. The Department did open the Florence street location in North Omaha on Tuesday, July 21, 2009, in the morning to process any walk-in customers to ensure the system was working as anticipated. All 13 locations were reopened for business on Wednesday, July 22, 2009.

Exhibit A

STATE OF NEBRASKA INFORMATION TECHNOLOGY SYSTEMS

DEPARTMENT OF MOTOR VEHICLES DRIVER LICENSING SYSTEM IMPLEMENTATION ISSUE

The Department did incur some additional costs due to this event. Most of the additional costs were for overtime of employees who were working around the clock trying to get the system up and running. The Department is working with their legal counsel to consider possible ways to recover some of the extra costs. The majority of this project is funded through cash fund appropriation authorized by 2008 Neb. Laws LB 911 with additional funds provided through a Federal grant.

The Department does have a disaster recovery plan that is up-to-date. The Department does not intend on changing anything in order to prevent something like this from happening again because this was such a strange chain of events. It was determined there would be nothing the Department could do to prevent this from happening in the future.

Exhibit B

STATE OF NEBRASKA INFORMATION TECHNOLOGY SYSTEMS

DEPARTMENT OF HEALTH AND HUMAN SERVICES
MMIS CONTRACT TERMINATION

Per the United States Department of Health and Human Services – Centers for Medicare and Medicaid Services (CMS), for Medicaid purposes, the mechanized claims processing and information retrieval system which Nebraska and other states are required to have is the Medicaid Management Information System (MMIS). MMIS is an integrated group of procedures and computer processing operations developed at the general design level to meet principal objectives such as the Title XIX program control and administrative costs, service to recipients, providers and inquiries; operations of claims control and computer capabilities; and management reporting for planning and control.

In October 1972, Public Law 92-603 was enacted in which Section 235 provided for 90% Federal Financial Participation (FFP) for design, development, or installation, and 75% FFP for operation of State mechanized claims processing and information retrieval systems approved by the U.S. Department of Health and Human Services Secretary.

Federal regulations requiring more detailed reporting relating to Medicaid must be implemented by 2013. As a result of the updated requirements needed, many states are in the process of replacing or updating their MMIS. To comply with the Federal regulations, the State of Nebraska’s Department of Health and Human Services (DHHS) through the Department of Administrative Services State Purchasing Bureau issued a Request for Proposal (RFP) on December 15, 2005. All bids were rejected on June 20, 2006. A second RFP (2017Z1) was issued on May 2, 2007, with 3 companies issuing proposals. On November 21, 2007, a letter of intent to award the contract to FourThought Group, Inc. (FTG) was issued.

DHHS contracted with FTG to provide the design, development, implementation, certification, and maintenance and support of a new MMIS for the period effective May 1, 2008, through November 30, 2012, with the option to renew for 3 additional years for maintenance and support. The total contract was for $70,478,106. A portion of the total contract was for maintenance and support beyond 2012, the total for the time period of May 1, 2008, through November 30, 2012, was $45,087,674.

In July 2009, DHHS terminated the contract with FTG because the company could not deliver the system as needed. On August 21, 2009, DHHS signed a settlement agreement with FTG which required DHHS to pay FTG a total of $4,750,000. Below is a table showing the payments made to FTG during the contract period and the settlement. Payments to FTG were paid with Federal funds (90%) and State Funds (10%).

	DHHS Cash/MMIS Fund (State Funds)	Federal Funds	Total Payments
Payments to FTG July 2008 through June 2009	$ 688,118.85	$ 6,193,069.77	$ 6,881,188.62
Settlement Payment in August 2009	475,000.00	4,275,000.00	4,750,000.00
Totals	$ 1,163,118.85	$ 10,468,069.77	$ 11,631,188.62

Exhibit B

STATE OF NEBRASKA INFORMATION TECHNOLOGY SYSTEMS

DEPARTMENT OF HEALTH AND HUMAN SERVICES

MMIS CONTRACT TERMINATION

DHHS has finalized documents to CMS to identify and explain termination of contract. CMS has been provided details of deliverables received from FTG to support payments. DHHS has indicated that while the Federal government may not seek reimbursement for this contract; it may impact future Federal dollars as related to subsequent approval for similar work products.

When asked, "What specific values/deliverables did the State get from FTG for the money spent?" DHHS provided the following response: "The deliverables paid under this project fall under two categories: those that provided value during and within the context of the project and those that provide a valuable basis for future work products. Within the context of the project, deliverables such as the work plan, schedule, status reports, and project control, quality management and project management plans were necessary for management of the project. Additional deliverables such as the deployment, testing, development and configuration management plans and environments provided value primarily tied to the specific solution proposed in the project (e.g., the technical architecture and environment), although in some cases, also provide useable information in any context. Other deliverables such as the requirements validation, business process descriptions, gap analyses, and data conversion plans and products contain useful information and will provide a basis for future work products."

When asked, "What DHHS plans to do to meet the requirements of the Feds," DHHS provided the following response: "Throughout the project and during closure activities, DHHS communicated with officials from the Centers for Medicare and Medicaid Services (CMS). A request for federal funding for planning and preparation activities has been submitted to CMS. Planning will include strategies to meet existing federal mandates and will provide the opportunity to incorporate recent state and federal initiatives and reforms such as health information technology/health information exchange."

As of the date of this report, DHHS is still waiting on confirmation of acceptance or denial of the above noted plan and verification that the Federal government will not seek reimbursement of the Federal funds spent on the contract with FTG.