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.nebraska.gov

February 10, 2014

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

Dear Ms. Decker:

We have audited the basic financial statements of the State of Nebraska (State) as of and for the year ended June 30, 2013, in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and have issued our report thereon dated December 30, 2013. In planning and performing our audit, we considered the State's internal control over financial reporting (internal control) as a basis for designing audit procedures for the purpose of expressing our opinions on the basic financial statements of the State, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

In connection with our audit described above, we noted certain internal control or compliance matters related to the State's Information Technology (IT) for select applications administered by the Department of Administrative Services – Office of the Chief Information Officer (OCIO) and State agency management, or other operational matters that are presented below for your consideration. These comments and recommendations, which have been discussed with the appropriate members of the OCIO's management, are intended to improve internal control or result in other operating efficiencies.

Our consideration of internal control included a review of prior year comments and recommendations. To the extent the situations that prompted the recommendations in the prior year still exist, they have been incorporated in the comments presented for the current year. All other prior year comments and recommendations (if applicable) have been satisfactorily resolved.

Our consideration of internal control was for the limited purpose described in the first paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified.

Draft copies of this letter were furnished to the OCIO to provide management with an opportunity to review and to respond to the comments and recommendations contained herein. All formal responses received have been incorporated into this letter. Responses have been objectively evaluated and recognized, as appropriate, in the letter. Responses that indicate corrective action has been taken were not verified at this time but will be verified in the next audit.

Background

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

Neb. Rev. Stat. § 86-515 (Cum. Supp. 2012) created the Nebraska Information Technology Commission (NITC). That body consists of nine voting members, including the Governor of Nebraska or his or her designee, and one ex officio, nonvoting member appointed from the Transportation and Telecommunications Committee of the Legislature by the Executive Board of the Legislative Council. The duties of the NITC are defined by Neb. Rev. Stat. § 86-516 (Cum. Supp. 2012) and include adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel.

The Commission is currently comprised of the following members:

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

The OCIO works with the NITC to ensure cost-effective and efficient use of State resources and investments in information technology. The OCIO assists 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 the resulting NITC standards and guidelines, unless they request and are approved for a waiver of the standard or guideline from the technical panel, or are noted as being specifically excluded in policy. The OCIO and NITC work closely with State agencies to meet their respective statutory requirements.

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

Department of Administrative Services (DAS):

- ***Active Directory*** **–** Active Directory is a directory service application used to authenticate and authorize users and computers on the State's network. It also provides security policies over computers, users, and groups. The Auditor of Public Accounts (APA) audited the State domain provided by the OCIO as a shared service; however, several other agency domains existed.

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

- ***OnBase*** **–** OnBase is an Enterprise Content Management (ECM) document imaging system utilized by 14 State agencies and political subdivisions to centralize their important business content electronically in one location. OnBase allows agencies to establish automated workflows for business processes. The system was purchased with the intent for State agencies to go paperless.

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

- ***Workday –*** This application is responsible for processing the human resource business processes for the State of Nebraska. Data interfaces with EnterpriseOne.

Nebraska Department of Education (NDE):

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

- ***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.

- ***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.

Department of Health and Human Services (DHHS):

- ***Med-IT*** – The Med-IT application supports the Every Woman Matters Program and Wise Woman Programs. These programs are Federally funded by the Center for Disease Control and Prevention (CDCP). They provide breast and cervical cancer screening to women ages 40 to 74, and cardiovascular and diabetes screening to women ages 40 to 64. The application is used to determine program eligibility, manage client health records, calculate payments to providers, and create reports for the CDCP.

- ***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 applications, including EnterpriseOne.

- ***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 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.

- ***Food Distribution Program (FDP)*** – This application allows authorized users to order/request commodities (see WBSCM below) from the State based on their portion of the annual entitlement.

- ***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.

- ***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 invoicing. MDR interfaces with MMIS to receive claims data to calculate rebateable units, as well as with the Centers for Medicare and Medicaid Services (CMS) to receive rebate amounts, per the National Drug Code (NDC), to create amounts for invoicing. MDR also sends utilization of NDCs to the CMS.

- ***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.

- ***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.

- ***Web-Base Supply Chain Management (WBSCM)*** – This application is for use in the Food Distribution Program. It is a Federal off-the-shelf ERP system that allows the State to place orders for commodities based on an annual entitlement. In addition, this application allows the State to track and store any commodities purchased from the Federal program.

- ***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.

Department of Labor:

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

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

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

Nebraska Lottery, Department of Revenue:

- ***Internal Control System (ICS) –*** ICS independently validates and balances the online and instant games system results.

- ***GTECH –*** GTECH is the vendor providing a unified lottery system for instant (scratch) and online (e.g., Powerball®) tickets.

Department of Motor Vehicles (DMV):

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

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

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

Nebraska Public Employees Retirement Systems (NPERS):

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

Department of Roads:

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

Supreme Court:

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

State Records Board:

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

The following are the comments and recommendations for the year ended June 30, 2013, related to the State of Nebraska IT Systems controls. It should be noted this letter is critical in nature, as it contains only our comments and recommendations on the areas noted for improvement.

COMMENTS AND RECOMMENDATIONS

1. Developer Access to Production Environment

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.3.2.3, Separation of Duties, states:

> *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.*

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

Two DDS application developers and one DDS contracted developer at the Department of Education had full access to the production environment.

A similar comment was noted in the prior year management letter.

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

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

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

The Department of Education responded: We are not contesting this finding and are planning no action on this item.

2. Access Commensurate with Job Responsibilities

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, states:

> *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 (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 4.7.3, Privileged Accounts Management, 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.*

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.3.2.3, Separation of Duties, states:

> *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.*

The Supervisor's Guide – NFOCUS Role Based Access Profile Assignment for Internal Staff, states, in part:

> *Access to N-FOCUS is based on the job tasks performed by the individual. The direct supervisor must complete, sign, and submit the N-Focus Access Request Checklist before appropriate access will be assigned. Use of the checklist is required for new hires as well as when there is a change in assigned duties.*

That same document also provides:

> *Each job activity corresponds to a defined access role in the N-FOCUS system. By checking the appropriate job activity or activities, the individual will be assigned the appropriate N-FOCUS access role(s).*

Finally, the Supervisor's Guide points out:

> *To meet state and federal security safeguard requirements, each individual with access to N-FOCUS must have their access level reviewed on an annual basis.*

A good internal control plan includes utilizing logical access controls to ensure user access is commensurate with specific job responsibilities. A good internal control plan also includes maintaining documentation of application roles that identifies the access each role provides a user.

- One DHHS contracted application developer had "ALTER" access to an NFOCUS dataset that was not required for his job duties.

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

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

- One Department of Labor contract employee did not require super user access to EnterpriseOne. That access allowed the contractor to circumvent controls, view confidential data from other agencies, and modify user account security statewide. According to the EnterpriseOne administrative team, they were ordered by the Director of the DAS to allow the access against their best judgment. The contractor's access began on May 9, 2012. Furthermore, the user granted himself the ability to approve and post all of the Department's accounting transactions by assigning the Department of Labor's Director of Financial Services ID to his own.

- One DHHS WIC application user had access to two roles, when only one was appropriate. Due to a lack of documentation to support the level of access each WIC role granted, DHHS could not identify the differences between the roles.

- Three Department of Labor BPS application users had access to supervisor roles, which were not necessary for their job responsibilities. The supervisor roles provided the ability to maintain or modify other users' access within BPS.

- Four Department of Labor TMS application users had access to a Labor mainframe superior group, which was not necessary for their job responsibilities. Any datasets tied to the superior group could be inappropriately accessed.

- Eight DHHS NFOCUS profiles allowed users to create an organization, create a service approval, create a service authorization, and enter a claim for payment. In addition, one of the eight NFOCUS profiles also had the ability to preprint and adjust claims; that group had 94 users connected to it.

- One of 20 DHHS NFOCUS application users tested had access that was unnecessary for her job responsibilities. The user had retained that access from a previous position that was no longer needed.

- The established DHHS process for assigning NFOCUS access to users was not followed. The NFOCUS Access Request Checklist was not properly completed for two of five users tested. In addition, users were granted more access to NFOCUS than requested on three of four checklists tested.

- One Department of Education employee had the ability to approve both CACFP applications and claims in the CNP application for daycare homes.

A similar comment was noted in the prior IT management letter.

When an individual has access beyond what his or her job responsibilities require, there is an increased risk for unauthorized changes or transactions that could result in the loss of State funds. When no review is performed to ensure users do not have unwarranted access to applications, there is an increased risk for unauthorized changes to the system. Without current documentation of application security roles, there is an increased risk inappropriate access will be granted to a user. When a proper segregation of duties is not established through application security roles/profiles, there is an increased risk for unauthorized claim payments and a loss for State and Federal funds. Users who are improperly granted the ability to make changes to system security parameters may cause unapproved changes to be implemented. If such access is not implemented and configured properly, business cycle controls may be ineffective. When users are granted inappropriate access, significant information resources may be modified inappropriately, disclosed without authorization, and/or unavailable when needed.

We recommend:

- All application owners adequately review a list of users on a periodic basis to verify access levels are appropriate based on job responsibilities of the employees.
- Reviewing application roles/profiles and assigned access to ensure there is a proper segregation of duties around the claims payment process.
- Removing user access that is not required for their job responsibilities or that causes a lack of segregation of duties.
- Obtaining and maintaining application security role documentation to ensure access granted is in line with management's intentions.
- Reviewing established procedures to ensure access checklists are properly completed, maintained, and reviewed annually or when there is a change of assigned duties.

OCIO's Response: The Office of the CIO will continue to work with the agencies identified to establish a review schedule of all users of applications to verify access levels are appropriate. The OCIO will continue to refine our internal process to assist in agency reviews of mainframe access at least annually

to ensure that access levels are appropriate. Additionally, individual agency responses are offered below:

The Department of Education responded: The CNP user ID that had access to approve application and claims has been corrected. The rights to approve claims has been removed.

The Department of Health and Human Services responded: The Department will review its processes and procedures to approve and review user access to the Department's Information technology applications.

The Department of Labor responded: NDOL did not have access to this information and the super user status in EnterpriseOne was not requested by NDOL. The auditor alerted DAS prior to having a conversation with NDOL, and access was removed for the person in question. Regarding the roles of employees set up with supervisor roles, UI Benefits does not agree with this finding. UI Benefits employees are required to have temporarily enhanced levels of access to properly and efficiently complete the functions of their job. BPS contains a "bundling" feature for access control. Supervisor roles contain functional access necessary for some non-supervisors to complete their job functions, often on a temporary basis. As a compensatory control, all access changes are reviewed monthly by Internal Security for proper access control and functional requirement. Anomalies are questioned and documented. Thus, if a non-supervisor were to attempt a functional role modification of another user, Internal Security would identify that transaction and investigate the activity. Internal Security will develop and implement a functional security report to review all active users to ensure all terminated employees have had user access removed and application users have access necessary for their job responsibilities.

APA Response: The ability to modify other users' access should be restricted to only those users who need to do so on a regular basis in the performance of their specific job functions. The Department has previously documented its agreement with this finding. It is inexplicable, therefore, why the Department now disagrees with that same finding and chooses not to make the appropriate changes to its current procedures.

The Department of Motor Vehicles responded: The Department of Motor Vehicles performs periodic review of user and access levels and removes access or capabilities when the user no longer requires the access to perform their job. Programmers/developers employed by the CIO have historically and will continue to be an integral part of our daily operation and are granted authority to DMV applications and systems to ensure services are provided to our customers without interruption.

3. Terminated User Access

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, states:

> *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 (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.*

Nebraska State Accounting Manual, AM-005, General Policies, Section 32, Terminated Employee EnterpriseOne ID's, states, in part:

> *Each agency shall have a documented procedure to immediately disable the EnterpriseOne ID of an employee who has terminated employment with the agency. It is the responsibility of the agency's authorized agent to request termination of the User ID from the computer system within five working days from the termination date . . . .*

A good internal control plan includes a process to ensure terminated users' access is removed timely.

- For 4 Supreme Court employees, 22 County employees, and 4 City employees who terminated employment, access to the JUSTICE application was not removed in a timely manner (within 3 business days). In addition, despite having terminated, one contracted programmer still had an active user ID for the software used to move changes to the JUSTICE production environment.

- For 12 of 21 users tested from a DHHS external contractor, access to the MMIS application was not removed after termination. DHHS maintained a manual listing of MMIS external users; however, the list was not kept current. The Excel file was maintained by one person and included over 1,000 worksheets, one for each external entity with MMIS users.

- For one DHHS WIC application user, access to the application was not removed after her termination on July 23, 2012. WIC did maintain a manual listing of terminated users; however, the list was not kept current.

- For five Department of Labor BPS terminated users, access to the application was not removed as of May 2013. Termination dates ranged from March 2010 to March 2013. None of the users accessed BPS after their termination dates.

- For two Department of Labor TMS terminated users, access to the application was not removed as of April 2013. The termination dates of the users were unknown. They last logged into the application in 1992 and 2001.

- For one NEworks user no longer employed by the WIA contractor, access to the application was not removed after termination. The user terminated employment with the contractor in September 2011. The user did not access the application after the termination date.

- For 20 of 24 terminated EnterpriseOne users, functional access to the application was not removed in a timely manner (within 3 business days). In addition, five of those IDs accessed EnterpriseOne after the user terminated.

- For 6 of 12 DHHS internal FDP application users, access to the application was not removed when the users were no longer employed by the FDP division.

- For 41 of 43 DHHS external FDP application users, access to the application was not removed when they no longer required access to the system.

- There was no process to ensure Department of Education GMS district administrator accounts were removed in a timely manner upon termination (within 3 business days). The school districts were responsible for informing NDE of terminated administrators; however, the accounts were not being monitored or reviewed by NDE on a periodic basis.

- For one of five terminated Department of Education employees tested, Network Services was not notified of the contract employee's termination and access was not removed in a timely manner (within 3 business days).

A similar comment was noted in the prior IT management letter.

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

> We recommend application owners review user access on a periodic basis to ensure access is appropriate. Additionally, a formalized process to remove access to applications and networks should be established and followed, including communication with external parties on the importance of notifying the State of terminations so access can be removed in a timely manner. A terminated user's access should be removed immediately. We recommend educating users on the termination process in Workday and encouraging them to enter termination dates as soon as they are identified. The creation, modification, and removal of a user's access should be documented and include a date stamp.

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

The Department of Administrative Services/Accounting Division responded: State Accounting will continue to educate agencies on the termination process of an employee and review internal controls.

The Department of Education responded: There can only be a single district administrator for each district in the NDE portal. Thus, when a new administrator is added to a district, the departed administrator's access is removed from all Portal collections for that district, including GMS. NDE staff have developed a security access guidance document that outlines who, what, when, where and how a vendor such as CNP can access NDE systems and the process vendors must use to obtain access. The security document further identifies appropriate NDE staff and time frames that a vendor must follow in order to access or have software installed on an NDE system.

The Department of Health and Human Services responded: The Department will review its processes and procedures related to terminating user access to information technology applications. This will include reviewing processes and procedures related to information technology applications not currently being support by the Department's Information Systems and Technology Section.

The Department of Labor responded: Management agrees in part with the Auditors findings; however, of the five active users in BPS, two were terminated since the implementation of the Access Request Process System (ARP) in ECM-On Base. ARP was designed and implemented to combat these oversights. However, requesting termination in the application does not terminate the user. ARP contains a workflow to document the creation and termination process and catalogs the documentation for storage and retrieval. UI Benefits Internal Security reviews the bi-weekly HR employee status change document to ensure status changes have a corresponding access change request form. ARP was created to strengthen the Department's access creation and termination process. These accounts appear to be well prior to the ARP process. Internal Security will develop and implement a functional security report to review all active users to ensure all terminated employees have had user access removed and application users have access necessary for their job responsibilities.

The Nebraska Supreme Court responded: There is an established internal process the Supreme Court follows. When an individual's employment is ended, the personnel manager notifies, in writing, AOC IT to remove their access to all state systems.

4. Shared IDs

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.7.3, Privileged Accounts Management, states, in part:

> *All individuals requiring special privileges (programmers, database administrators, network and security administrators, etc.) will have a unique privileged account (UserID) so activities can be traced to the responsible user.*

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.3.1, Individual Accountability, states, in part:

> *Each user must understand his/her role and responsibilities regarding information security issues and protecting state information. Access to agency computer(s), computer systems, and networks where the data owner(s) has authorized access, based upon the 'Principle of Least Privilege', must be provided through the use of individually assigned unique computer identifiers, known as UserIDs, or other technologies including biometrics, token cards, etc. Each individual is responsible for reasonably protecting against unauthorized activities performed with their UserID.*

When multiple users require the periodic use of system IDs, a good internal control plan includes an independent, documented review of the access to ensure accountability for changes to the system.

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

- We noted 18 generic IDs were shared among users to gain access to the Supreme Court's JUSTICE application. One of the generic IDs was utilized by the JUSTICE programmers to gain access to the JUSTICE production environment.

- The DHHS FDP staff allowed external FDP users to reuse IDs instead of assigning unique IDs for each new user.

- The Mainframe IDs of terminated DMV users were reissued to new employees.

A similar comment was noted in the prior IT management letter.

Without an independent documented review of system ID use, there is an increased risk of unauthorized changes being made without the ability of management to hold an individual accountable. Inadequate authentication procedures may lead to financial loss and operational damage through unintentional or deliberate unauthorized access, alteration, and use of information resources. Shared IDs make it difficult to identify the individual who accessed the computer system.

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

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

The Department of Administrative Services/Accounting Division responded: State Accounting will implement additional internal controls to ensure accountability for changes in the system when sharing system IDs to support EnterpriseOne.

The Department of Health and Human Services responded: The Department will review its processes and procedures related to user shared IDs to Information technology applications. This will include reviewing processes and procedures related to information technology applications no currently being supported by the Department's Information Systems and Technology section.

The Department of Motor Vehicles responded: The DMV is no longer reissuing user IDs and profiles to new employees.

The Nebraska Supreme Court responded: In coordination with the OCIO, all shared ID's have been eliminated with the exception of emergency ID's which can be activated by submitting a Help Desk ticket as needed.

5. Password Complexity

NITC Standards and Guidelines, Password Standard 8-301, Section 1.2, Minimum Password Complexity Construction, states, in part:

> *The following are the minimum password requirements for State of Nebraska passwords:*
> - *Must contain a minimum 8 characters . . . .*

Section 2 of that same standard states, in part:

> *All employees and contractors of the State of Nebraska shall use a password that follows at least a confidential level of authentication when logging into a state network or application.*

Additionally, Section 2.2 requires, as is relevant:

> *A password used to access confidential information must follow the password complexity rules outlined in section 1.2 and must contain the following additional requirement:*
> - *Expire after 90 days*

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.5.4, Clear Screen, states:

> *To prevent unauthorized access to information, agencies will implement automated techniques or controls to require authentication or re-authentication after a predetermined period of inactivity for desk tops, laptops, PDA's and any other computer systems where authentication is required. These controls may include such techniques as password protected screen savers, automated logoff processes, or re-authentication after a set time out period.*

A good internal control plan includes utilizing system parameters to enforce password and re-authentication rules that require users to comply with NITC standards. In addition, a good internal control plan includes the use of strong encryption methods when storing sensitive data, including passwords, to ensure they are not easily accessible to unauthorized users.

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

- The Department of Motor Vehicles VTR and MCS applications did not force users to meet the NITC password requirement for expiration of passwords. Twenty-five active MCS user IDs had non-expiring passwords. The APA tested 3 county VTR instances and noted 26 user IDs for Lancaster County, 25 for Sarpy County, and 25 for Sheridan County that had non-expiring passwords.

- The Department of Education GMS Portal login used by school districts did not force users to meet the NITC password requirement for expiration of passwords. Users were prompted every 90 days with the option to retain or change their password.

- The Department of Education CNP application did not force users to meet the NITC password requirement for expiration of passwords. The application allowed users to change their password once every 360 days.

- The Department of Labor BPS application did not force users to meet the NITC password requirement for length. The application setting for minimum password length was 6 characters. In addition, multiple generations of BPS passwords were stored in plain text, and were not properly encrypted.

- The Supreme Court JUSTICE application required a user to re-authenticate to the server after four hours of inactivity. While the standard does not define "predetermined period of inactivity", four hours seems unreasonable and inconsistent with the intent of the standard's goal of preventing unauthorized access to information.

- The Supreme Court JUSTICE application did not force users to meet NITC password requirements for length and complexity. It was also noted, for five counties tested, roughly 300 users at each county were not required to change their passwords periodically. See table below.

	Merrick	**Holt**	**Platte**	**Adams**	**Douglas**
User Group	**Number of Users**				
County Users	96	95	97	97	97
JUSPUBLIC (Public Access)	1	1	1	1	1
Supreme Court Employees	34	37	37	42	53
Generic Programmer ID	1	1	1	1	1
Other State Agencies	166	166	166	166	166
Total	**298**	**300**	**302**	**307**	**318**

A similar comment was noted in the prior IT management letter.

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

> We recommend adequate password complexity be implemented to ensure user compliance with NITC requirements. We also recommend passwords be properly encrypted. Finally, we recommend the Supreme Court sets its re-authentication facility to a more reasonable level.

OCIO's Response: The Office of the CIO will continue to work with agencies to ensure NITC compliance and/or exceptions will be document through the NITC process. Additionally, individual agency responses are offered below:

The Department of Education responded: Protocols and Process for requiring the password to be changed every 90 days are being developed and put in place.

The Department of Labor responded: The Department partially agrees with the finding. When developed in 2006, BPS was developed so that it could share the same Lightweight Directory Application Protocol (LDAP) with the Interactive Voice Response (IVR). Changing password requirements on the web application requires a separate LDAP for BPS as well as code changes within the application. Besides providing a pin, the user also provides their social security number in order to access their record. Associated records must match. The Department recognizes the importance of application security and has taken other measures to ensure security, such as installing tools and appliances that verify the security of the application code and monitor access to the application. Passwords for Department staff who access the application are NITC compliant. Regarding TMS, the Department does not control the passwords. The LABZ is assigned by OCIO. The Department is implementing a new front end that will provide access to both the BPS and NEworks applications. The front end will meet NITC authentication standards regarding password complexity and encryption. For users who do not come through the front end and log directly into the applications, the Department will research both the e-Directory and application sides to determine what changes need to be made to be compliant. The Department will also work with OCIO regarding TMS passwords.

The Department of Motor Vehicles responded: The DMV is now in compliance with the password complexity rules established by the NITC on the VTR and MCS systems. In reference to the non-expiring VTR passwords: The DMV IT Division and the DMV Driver and Vehicle Records Division require access to all of the county VTR systems to provide client support. To accomplish this service, the users with non-expiring passwords log in to the VTR State system (with user ids and expiring passwords) and then have the ability to 'pass through' to the county systems through a system to system authentication. It is those system to system user ids and non-expiring passwords that enable the required functionality. In reference to the non-expiring MCS passwords: The passwords designated as non-expiring are system to system passwords which enable system integration and law enforcement users that require 24/7 access without support from the DMV. It should be noted that the law enforcement users, prior to accessing the DMV system, would be required to authenticate to the State Patrol network.

The Nebraska Supreme Court responded: In coordination with the OCIO, all JUSTICE program users have passwords in compliance with the NITC complexity standards. The time-out standard for re-authentication to the server was not adjusted, as this impacts other agencies running programs on the AS400 and is not something the Supreme Court can determine.

6. Standardized Change Management Process

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.9.11, Key Management, states:

> *To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained. These change control procedures will apply to agency business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.*

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.3.2.3, Separation of Duties, states:

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.

A good internal control plan includes a formal methodology to guide the development of applications and systems. Changes to existing applications and systems should undergo initial evaluation, authorization, and implementation procedures to ensure they have met expectations and minimized user disruption. These processes should be adequately documented.

- The Supreme Court used a system known as JTrac to document the request, testing, and approval of changes to JUSTICE. Production changes to the JUSTICE application were implemented on 214 days of calendar year 2012. For 16 of 21 days of changes tested, the APA was unable to tie changes placed into production to an approved Service Request in JTrac. Additionally, there was no review of actual changes made by the programmers to ensure all changes made were appropriate and authorized.

- The DMV did not have formalized change management procedures in place to include a change request, test documentation, and management approval for all VTR and TSI changes. There was also a lack of segregation of duties surrounding the DMV change management process.

A similar comment was noted in the prior IT management letter.

Without proper and consistent change control standards and segregation of duties, changes to an application may be made without specific management approvals. This could lead to data loss, compromised financial data integrity, and unintended system down time.

We recommend the Supreme Court ensure the software utilized to make changes to the JUSTICE application traces to the JTrac change management system maintained to document the request, testing, and approval of changes. Additionally, we recommend the Supreme Court periodically obtain and review a report of JUSTICE changes from the OCIO to ensure changes made were appropriate and authorized. We also recommend DMV develop and implement a formalized change management process for MCS, VTR, and TSI applications. The process should include documented change requests, testing procedures, and approval to implement the change into production. Finally, we recommend DMV implement an adequate segregation of duties to prevent a single user from checking out code, developing, and promoting changes to the point where the OCIO moves the change to production.

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

The Department of Motor Vehicles responded: The organizational structure and interactions of the IT Division within the DMV have been developed to maximize resources and operational efficiency while mitigating the associated risks. The DMV IT Division works directly with Division Administrators. All database and application changes are performed only at the request of the Division Administrator that

owns the data and process. All database and application changes are tested and approved by the authorized division prior to implementation.

The Nebraska Supreme Court responded: JUSTICE program change management is handled through the OCIO Implementer system. JUSTICE uses the JTRAC system to manage change requests and approvals. When program changes are moved to production the Implementer code is logged to JTRAC to make changes traceable between systems.

7. System Monitoring

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.7.10, Monitoring System Access and Use, 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.*

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

The Department of Roads did not review the security alert logs set up for the Windows environment. In addition, the RBS application did not have the capability to record which user completed each element of the receipting process for subsequent review.

A similar comment was noted in the prior IT management letter.

Without monitoring system event logs, there is an increase risk for damage to operating systems and physical hardware. There is also a lack of accountability when accounting records cannot be tied to the user who performed them.

> We recommend the Department of Roads perform a documented review of necessary system event logs and violation reports to detect unauthorized events or system failures. We also recommend the Department of Roads establish controls to capture the user ID used to complete each phase of an accounting process.

OCIO's Response: The Office of the CIO will continue to work with the Department of Roads to resolve the issue identified and ensure the production environments are protected. Additionally, the Department of Roads offered the response below:

The Department of Roads responded: We had to resolve a couple of issues in regard to the review of security alert logs but feel that we can have this in place within a month. Roads will contact the OCIO on March 3rd, 2014 to update on their progress. The RBS application has been upgraded to contain the following data for each receipt; 1. Userid, Date, Time of initial entry. 2. Userid, Date, Time of Updated by. 3. Userid, Date, Time of Authorized by. 4. Userid, Date, Time of batched by.

8. Business Processes

A good internal control plan includes procedures to ensure the correct exemption rates are used for garnished wages.

DAS did not use the correct tables when calculating employee wage garnishments for delinquent State taxes. Instead, the agency used the Federal exemption amounts, which did not agree to the Nebraska rates.

A similar comment was noted in the prior IT management letter.

When the correct table for calculating garnishments for delinquent State taxes is not used, the employee's pay is calculated incorrectly.

> We recommend DAS work with Oracle to add an additional table for the State exemptions for State tax levies.

OCIO's Response: The Office of the CIO will work with the Department of Administrative Services when requested to address this business need. Additionally, the DAS response is offered below:

The Department of Administrative Services/Accounting Division responded: State Accounting is conducting an upgrade of EnterpriseOne to 9.1 in 2014 which includes the additional table required for the State exemptions for State tax levies.

9. Business Continuity

NITC Standards and Guidelines, Information Technology Disaster Recovery Plan Standard 8-201, Section 1, Standard, 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.*
>
> *The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency. The following elements, at a minimum, must be included:*
> - *Identification of critical computer systems and services to the agency's mission and business functions.*
> - *Critical systems and services preservation processes and offsite storage strategy and methods to protect storage media . . . .*
> - *Annual plan review, revision, and approval process.*

Additionally, NITC Standards and Guidelines, Information Technology Disaster Recovery Plan, Standard 8-201, Section 5.2, Agency and Institutional Heads, states:

> *The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing disaster recovery/business continuity programs consistent with this standard. The authority may delegate this responsibility but delegation does not remove the accountability.*

IT Governance Institute's Control Objectives for Information and Related Technology (COBIT) 4.1 DS4 Ensure Continuous Service, states, in part,

> *The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilizing offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimizes the probability and impact of a major IT service interruption on key business functions and processes.*

- The OCIO did not review and update its COOP/Disaster recovery plans for the fiscal year tested. Contact lists were last updated in July 2011. COOP/disaster recovery plans were last updated in January 2012.

- The contracted programming support for the DMV MCS application consisted of one individual with both the business knowledge and programming skill set required to support the application. DMV had no backup plan should the programmer become unavailable. This was also an issue for the VTR application.

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

A similar comment was noted in the prior IT management letter.

When COOP/Disaster Recovery plans are not reviewed and updated periodically, there is an increased risk that procedures and contact lists will be out of date. When only one person is trained to support an application, there is an increased risk services supported by the application may be disrupted for a prolonged period of time. When backup tapes are not maintained off-site, there is an increased risk for the loss of data or prolonged system down time.

> We recommend the OCIO review the COOP/Disaster Recovery plans annually and make any necessary revisions. We recommend DMV evaluate the risks associated with relying on one individual to provide application support and consider training or hiring additional staff to support the MCS and VTR applications. We recommend the Supreme Court require the Counties to store backup tapes off-site to ensure effective data retention.

OCIO's Response: The Office of the CIO has recently filled the COOP/Disaster Recovery position within the organization. This individual has been tasked with getting the annual review of the OCIO plan back on track with an annual review. The OCIO will continue to work with agencies to establish formalized business continuity plans with effective data retention testing and storage. Additionally, individual agency responses are offered below:

The Department of Motor Vehicles responded: The DMV is aware of the risk associated with not having duplicative staff for each functional area. To begin the mitigation of this risk, the DMV is developing a strategic business plan that will outline future projects and define the specific need and skills required for the additional application development staff for all functional areas.

The Nebraska Supreme Court responded: Server consolidation is ongoing to bring most of the courts on to virtual servers housed at the 501 building. Those court backups are done by the OCIO. Counties where the AS400 server has not been moved to a consolidated server are monitored by OCIO staff and are contacted if backups are not done. In some counties it is not the court office performing these backups. Court offices have been informed that backup tapes must be stored off site.

10. Edit Checks

NITC Standards and Guidelines, Information Security Policy Standard 8-101, Section 4.9.4, Input Data Validation, states:

> *An application's input data must be validated to ensure it is correct and appropriate including the detection of data input errors. The checks that are performed on the client side must also be performed at*

the server to ensure data integrity. Checks will be performed on the input of business transactions, static data (names, addresses, employee numbers, etc.) and parameter tables. A process should be set up to verify and correct fields, characters, and completeness of data and range/volume limits.

Best practices regarding audit record content are set out in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Auditing and Accountability Control AU-3, Content of Audit Records, states:

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g. the security state of the information system after the event occurred.)

A good internal control plan includes maintaining appropriate edit checks to ensure adequate transaction detail is required to post accounting transactions. A good internal control plan also requires proper monitoring of the overriding of edit checks. Furthermore, a good internal control plan also requires a limited number of individuals with supervisory duties having access to override or force pay claims.

- The APA identified 143 business units without an object account code that transactions could be posted to in EnterpriseOne.

- The DHHS NFOCUS application contained a service authorization edit check that could be overridden, and no monitoring procedures were in place to determine how often the edit was overridden, or who performed an override. Staff members were required to obtain approval for an override, but there were no controls in place to prevent a user from completing a service authorization without approval. In addition, the ability to force pay claims that were suspended due to an edit check was granted to individuals with non-supervisory duties, such as data entry operators and case aides.

- One of 13 Department of Education CNP application error codes tested did not set as expected. The edit was intended to prevent multiple claims with a submission type of "exception" from being paid in a 36-month period to a child care center.

- The cancelling penalties (CP) process in the Department of Labor's TMS application allowed staff to override penalties, leaving no audit trail in the system. Representatives who were permitted to collect monies in the field had this override ability.

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

We recommend State agencies work to ensure proper edit checks are in place and perform periodic reviews to ensure that these edit checks are functioning properly and not being inappropriately overridden. In addition, we recommend DHHS assign the ability to force pay claims only to supervisors who are able to review and determine the

appropriateness of overriding the claim edit check. Finally, we recommend the Department of Labor evaluate the need for the CP process, implement procedures to track its use, and periodically review user access to the process to ensure it is necessary and appropriate.

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

The Department of Administrative Services/Accounting Division responded: The 143 business units identified were reviewed and resolved.

The Department of Education responded: NDE has worked with the developer and the business rule, 528 has been corrected.

The Department of Health and Human Services responded: The Department will review its processes and procedures related to edit checks contained in the DHHS NFOCUS application.

11. Nebraska Interactive Contract, Addendums, and Agency Review

The State of Nebraska Service Contract with Nebraska Interactive, Section III, FF, states, in relevant part:

> *1a. Contractor on behalf of the State shall negotiate with and submit to the State for final approval written agreements from each separate data providing/collecting entity (hereinafter, "DP/CE") with which electronic communication is desired . . . .*
>
> *1b. Through addenda to this RFP and/or through the separate DP/CE contracts, Contractor and State Shall, by mutual agreement establish charges for, if appropriate, and other conditions of such access or collections with each DP/CE.*
>
> *1c. Such agreements or addenda to this RFP, if any, shall provide 1) for the costs DP/CEs will charge, which will be paid as expense by Contractor from the Network revenue account for information access or collection, 2) the time period and means by which DP/CEs will be paid from the Network revenue account for access or collection . . . .*
>
> *1e. After negotiating any separate DP/CE agreement, the agreement shall be presented by Contractor to NSRB for formal approval.*

Sound business practices and a good internal control plan require that procedures be in place to review amounts collected and remitted by a third party, as well as amounts charged for the collection of those receipts, to ensure the correct amounts are received or charged.

- DMV Teen Driver Permit Application services may be paid online through the DMV website; however, no addendum providing for the payment of such fees to the DMV and Nebraska Interactive was available.

- The $30 application fee for personalized message license plates in the Electronic Government Service Level Agreement (EGSLA) with the DMV conflicted with the $40 fee required under Neb. Rev. Stat. § 60-3,119 (Cum. Supp. 2012). Despite the incorrect fee listed in the agreement, the correct amount was actually collected.

- The $75 driver's license reinstatement fee in the EGSLA with the DMV conflicted with the $50 or $125 fees required under Neb. Rev. Stat. § 60-505.02 (Reissue 2010), Neb. Rev. Stat. § 60-4,100.01 (Reissue 2010), Neb. Rev. Stat. § 60-499.01 (Reissue 2010), and Neb. Rev. Stat. § 60-694.01 (Reissue 2010). The fees actually charged agreed to State Statute.

- The EGSLA with the DMV listed the fee for renewing or duplicating a driver's license at $26.50 and the fee for renewing or duplicating a State identification card at $13.50; however, per Neb. Rev. Stat. § 60-4,115 (Cum. Supp. 2012), the fees are the same for a standard Class O or M driver's license and a State identification card. The fees actually charged agreed to State Statute.

- DMV Addendum Six, which relates to driver's records, noted a fee of $3; however, as allowed by Neb. Rev. Stat. § 84-712 (Cum. Supp. 2013), an additional $1 fee is charged if a certified copy of the driver record is provided. That additional fee was not addressed by the addendum.

- Signed copies of DMV Addendum Eight (Message and Spirit Plate Fees), DMV Addendum Seven (Reinstatements), and the EGSLA with the DMV for International Fuel Tax Agreement (IFTA) were not on file. However, the fees noted in the EGSLA were being charged by the DMV and Nebraska Interactive.

- An additional $1 fee for transcripts (copies) of certified driver records was deposited in the General Fund instead of the DMV cash fund. The additional $1 fee was allowed per Neb. Rev. Stat. § 84-712(3) (Cum. Supp. 2013).

- The $10 fee listed for birth certificates under Attachment 1 of DHHS Addendum 1 conflicts with the $12 fee established under Neb. Rev. Stat. § 71-612(7) (Reissue 2009). Despite the incorrect fee listed in the addendum, the correct amount was actually collected.

- The Secretary of State did not review monthly reports from Nebraska Interactive to ensure the amounts received were proper. Additionally, that office was not aware of whether its information system tracked when a search or filing was done through Nebraska Interactive. In addition, we noted that no one reviewed the Nebraska Interactive report to ensure fees charged were in compliance with the agreement. Due to a miscalculation on the November 2012 payment statement, Nebraska Interactive overpaid $567 to the Secretary of State.

When amounts charged do not agree to service level agreements, or service level agreements are not signed/approved, confusion is created about appropriate fees. Moreover, fees not deposited in the DMV cash fund, as authorized, are not available for that agency's use. Without a review of the support for Nebraska Interactive receipts and charges, there is an increased risk the Secretary of State will not receive the correct amount under the contract, and the public may be charged an incorrect fee for services provided.

We recommend that all fees charged under the Nebraska Interactive contract agree to both any corresponding service level agreements and State statute. In addition, we recommend any addenda to that contract be appropriately signed and approved prior to fees being charged. Finally, we recommend the implementation of procedures for reviewing the accuracy of amounts submitted to the Secretary of State as receipts and fees charged by Nebraska Interactive.

OCIO's Response: The Office of the CIO will work with agencies when requested to address this business need. Additionally, individual agency responses are offered below:

The Department of Health and Human Services responded: The Department will review the document noted in the audit and make any changes deemed necessary.

The Department of Motor Vehicles responded: The DMV in partnership with Nebraska .GOV has created and/or updated the contract addendums between the State Records Board, Department of Motor Vehicles and Nebraska .GOV to clarify the issues listed above. The DMV will be presenting the addendums for approval by the Records Boards at the February 2014 meeting. Additionally, the "… additional $1 fee for transcripts (copies) of certified driver records that had been deposited in the General Fund instead of the DMV cash fund…" error has been corrected and procedures have been adopted to better monitor fee distributions.

The Secretary of State responded: The agency agrees with the recommendation and will implement procedures to more thoroughly review amounts received from Nebraska Interactive from Business Services' on-line filings and fees. With the current internal information system, an exact reconciliation may not be possible; however we believe an acceptable analytical review of revenues, filings and searches can be performed for reasonableness. The agency anticipates replacing the current Business Services information system within the next two bienniums. Any such replacement system will incorporate appropriate checks and balances to ensure that on-line filings can be reconciled with the internal accounting/filing records. As noted above, the Secretary of State will design and implement internal controls to ensure that on-line Business Services' fees collected by Nebraska Interactive are remitted to our agency. However, for other agencies, the Secretary of State's office is simply a conduit to distribute the funds collected. It is each agency's responsibility to design their own controls to ensure that all fees due their agency are remitted by Nebraska Interactive.

12. EnterpriseOne Timesheets

Neb. Rev. Stat. § 84-1001(1) (Reissue 2008) states:

> *All state officers and heads of departments and their deputies, assistants, and employees, except permanent part-time employees, temporary employees, and members of any board or commission not required to render full-time service, shall render not less than forty hours of labor each week except any week in which a paid holiday may occur.*

Sound business practices, as well as a good internal control plan, require hours actually worked by State employees to be adequately documented and such documentation to be kept on file to provide evidence of compliance with § 84-1001(1). Furthermore, a good internal control plan also requires employees who accrue vacation and sick leave to have adequate support that they actually earned the amounts recorded in their leave records.

Section 124-86, Payroll – Agency Records, of Nebraska Records Retention and Disposition Schedule 124, General Records, as issued by the Nebraska State Records Administrator, requires any "supporting records received or generated by an agency used to review, correct or adjust and certify agency payroll records" to be retained for five years. Per that same section, the supporting records may include timesheets and reports.

A good internal control plan requires approval of timesheets to be documented for subsequent review.

- Overtime exempt employees were not required to maintain a timesheet or other form of documentation to show at least forty hours were worked each week when using EnterpriseOne for time entry and leave exceptions. Exempt employees were only required to record leave used in the system.

- EnterpriseOne timesheets were not retained by the system for more than one year for two State agencies, and only the EnterpriseOne timesheet for the current pay period was retained by the system for other State agencies.

- Supervisors and human resource staff within the State agencies were able to change the employee's submitted timesheet without the employee's knowledge or documentation of the changes made.

- EnterpriseOne did not accurately track who approved timesheets in the system. Each employee is assigned a supervisor in his or her master file in the system. For State agencies that utilize timesheet entry in EnterpriseOne, the supervisor assigned to an employee approves the timesheet. However, supervisors are allowed to set up delegates in the system to approve timesheets in the supervisor's absence. The system does not record who actually approves the timesheet; if a delegate approves an employee timesheet, the system will record the assigned supervisor as the approver.

Without adequate records to support hours worked and approvals in the system, there is an increased risk for fraudulent or inaccurate payment of regular hours worked or accumulation of leave. A failure to retain important documentation risks noncompliance with Nebraska Records Retention and Disposition Schedule 124.

> We recommend DAS establish a policy requiring all employees of State agencies to maintain adequate supporting documentation, such as timesheets or certifications, in compliance with the Nebraska Records Retention and Disposition Schedule. Furthermore, we recommend DAS make the necessary changes to EnterpriseOne for the retention of timesheets, documentation of approvals, and changes to timesheets to ensure compliance with the Nebraska Records Retention and Disposition Schedule.

OCIO's Response: The Office of the CIO will work with the Department of Administrative Services when requested to address this business need. Additionally, the DAS response is offered below:

The Department of Administrative Services/Accounting Division responded: Exempt employees are required to only enter their leave exceptions into the EnterpriseOne time entry time keeping program. If there are no leave exceptions, the approving supervisor does not approve a time record and the system pays them standard hours. According to the Fair Labor Standards Act, exempt employees must receive the full salary for any week in which the employee performs any work without regard to the number of days or hours worked, unless certain exceptions are met. These allowable exceptions include certain deductions of one or more full days, but only if there is a bona fide plan, policy, or practice of providing compensation for a loss of salary. Additionally, exempt employees do not track, earn or receive overtime compensation for extra hours worked. These employees are paid a salary for performing the whole job and not for actual hours worked. However, they are required to record and seek approval for any leave exceptions or if they are in a leave without pay status. The two state agencies mentioned as not retaining time cards for more than one year refers to custom time card templates created for DEQ and Revenue. The system has been modified to retain the actual time card templates, as they were filled out by

employees, for more than one year. All time card data entered via Employee Self Service Time Entry is retained indefinitely in a time card work file. Reports are available to extract time card data for any pay period for which an employee entered time via ESS Time Entry.

13. Risk Assessment

NITC Standards and Guidelines, Information Security Policy Standard 8-101, Section 4.5.1, Physical Security Perimeter, states, in part:

> *Agencies will perform a periodic threat and risk assessment to determine the security risks to facilities that contain State information . . . .*

NITC Standards and Guidelines, Information Security Policy Standard 8-101, Section 4.9.3, Risk Assessment, states:

> *Security requirements and controls must reflect the value of the information involved, and the potential damage that might result from a failure or absence of security measures . . . . The framework for analyzing the security requirements and identifying controls to meet them is associated with a risk assessment, which must be performed by the data owner(s) and Agency management. A process must be established and implemented for each application to*
>
> - *Address the business risks and develop a data classification profile to understand the risks;*
> - *Identify security measures based on the criticality and data sensitivity and protection requirements;*
> - *Identify and implement specific controls based on security requirements and technical architecture;*
> - *Implement a method to test the effectiveness of the security controls; and*
> - *Identify processes and standards to support changes, ongoing management and to measure compliance.*

We noted the Department of Education did not complete a periodic risk assessment.

When no risk assessment is completed periodically, there is an increased risk that security vulnerabilities, which could have been prevented or monitored, will be exploited. This could cause downtime, loss of productivity, unauthorized access, or interference with State or Federal systems.

> We recommend the Department of Education complete a risk assessment on a periodic basis.

OCIO's Response: The Office of the CIO will continue to work with the Department of Education to complete a risk assessment. Additionally, the Department of Education offered the response below:

The Department of Education responded: NDE has a committee working to establish a Risk Management process and conduct annual Risk Assessments.

14. Address Book Numbers in EnterpriseOne

The State Accounting Manual, AM-005, Payments for State Employee Wages, states, in part:

> *In accordance with Statute 81-1117.05, payments for wages for all State employees will be by electronic funds transfer (EFT/Direct Deposit) . . . . State employees include all officers or employees of the state or any state agency and pursuant to Section 81-1178 shall include duly appointed members of committees, boards and commissions.*

A good internal control plan includes procedures to ensure that complete and accurate information is included for all active employees in order to assist in preventing the creation of fictitious employees,

erroneous benefits and fictitious vendors being paid, and to ensure taxable income can properly be reported (via IRS Form 1099).

- Twenty-two active EnterpriseOne address book numbers did not have an associated bank account noted. Of those active address book numbers, 16 Military Department employees had not received a paycheck in the last 5 years; 4 Per Diem employees had not received a paycheck of value in the last 5 years (paychecks processed each pay period equaled $0); and 2 Per Diem employees received a physical paper warrant paycheck each pay period.

- Twenty-one active employees had an inaccurate marital status listed in Workday. Those employees were categorized as "Single." However, their employee benefits noted a spouse as a dependent. A JUSTICE search was performed and found that none of the employees were involved in divorce proceedings with the spouse noted for benefits purposes.

- Fourteen employees had an incorrect name or social security number noted in EnterpriseOne.

- One Legislative Council employee had an incorrect original hire date and adjusted service date noted in EnterpriseOne. The employee had a break in service that was unaccounted for in EnterpriseOne.

- Eight vendor address book numbers lacked a mailing address in EnterpriseOne. Of those, one vendor had a mailing address noted in the name field.

- One public assistance address book number in EnterpriseOne had an inaccurate tax identification number.

- Thirty-six vendor address book numbers receiving payments in fiscal year 2013 had a tax identification number of "FOREIGN" noted in EnterpriseOne. In addition, three of those address book numbers had addresses located in the United States.

- One hundred and forty-five public assistance address book numbers receiving payments in fiscal year 2013 did not have an associated tax identification number noted in EnterpriseOne.

- Two hundred University of Nebraska vendor address book numbers receiving payments in fiscal year 2013 did not have an associated tax identification number noted in EnterpriseOne. Many of these vendor address book numbers appear to be international companies; however, some were individuals with addresses in the United States.

- Two address books numbers did not have a valid tax identification number. Those address book numbers were originally set up by Game and Parks for refunds; however, they were later used by other State agencies to make vendor payments.

- One active employee address book number in EnterpriseOne did not appear to be assigned to an actual employee and, therefore, should be removed.

Incomplete or inaccurate information related to active employees, vendors, or payees increases the risk of fraud or misuse of State funds due to potential fictitious payments, potential erroneous benefit payments, or potential tax consequences if taxable income is not properly reported.

> We recommend the State agencies update the necessary information for any active employees and vendors. We also recommend that the State agencies implement procedures to ensure that all active employee

address book numbers are associated with a valid name and tax identification number, as well as have an accurate mailing address, marital status, and bank account number.

OCIO's Response: The Office of the CIO will work with agencies when requested to address this business need. Additionally, the Department of Administrative Services response is offered below:

The Department of Administrative Services/Accounting Division responded: State Accounting will work with agencies as necessary to ensure Address Book records are adequately maintained.

15. Physical Access Security

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.5.1, Physical Security Perimeter, states, in part:

> *To detect and prevent unauthorized access attempts in areas within facilities that house sensitive or confidential information, where possible, agencies must utilize physical access controls designed to permit access by authorized users only that identify, authenticate and monitor all access attempts to restricted areas within agency facilities.*

- For 7 of 152 badges with access to an OCIO datacenter, access was not reasonable. Two ID's were generically named instead of being identified with a specific user. One badge was assigned to an employee who terminated on August 25, 2006. One badge was assigned to a State contractor no longer working at the State. Three badges were assigned to employees or elected officials who did not need the access to perform their job functions.

- Access to the DMV data center is restricted by a keypad with a key code; however, the key pad does not generate reports showing who accessed or attempted to access the data center.

Without appropriate security measures, including properly assigned access badges and the ability to generate reports indicating actual and attempted access, there is an increased risk of inappropriate or unauthorized individuals accessing the State's physical IT resources.

We recommend the State Patrol and OCIO work together to perform periodic reviews of access to the data centers and to limit such access to individuals who require it to perform their job functions. We also recommend the DMV consider discussing with Capitol Security various available security options. We recommend further the DMV develop procedures to periodically review access and attempted access to its datacenter.

OCIO's Response: The Office of the CIO will work with the APA on the specific ID's listed above, as well as continue to work toward an annual process to review access to the facility. The OCIO will also continue to work with state agencies to ensure that physical security to the OCIO data center and other IT environments appropriately restrict physical access. Additionally, the Department of Motor Vehicles response is offered below:

The Department of Motor Vehicles responded: The DMV will review security options available for the DMV datacenter.

16. Active Directory

A good internal control plan includes creating a reserve file to mitigate the effects of a Denial of Service (DoS) attack.

Best security practices and a good internal control plan include establishing the most secure policies, when practicable, to reduce the risk of a domain controller becoming compromised.

A good internal control plan includes running only essential services on servers, including Domain Controllers, to limit the possible points of attack a hacker could use to potentially gain access to state resources.

- During a review of the OCIO domain controllers, we noted a reserve file was not created to enable recovery from disk-space attacks.

- For 10 of 27 domain controller security policies reviewed, the value was not set as recommended for best security practices.

- The APA reviewed services running on the domain controllers and identified four services that were set to Automatic or Manual, and should be disabled.

When controls are not in place to mitigate the effects of a potential disk space attack, there is an increased risk of a prolonged directory service outage before returning to normal operations. When domain controller security policies are not set as recommend by best security practices, there is an increased risk an attacker could exploit a domain controller. When services not essential to normal domain controller functions are not disabled, those services increase the attack surface of the domain controller.

> We recommend the State perform a risk assessment and implement controls to mitigate potential threats, such as disk space attacks. We recommend the OCIO review domain controller security policies and running services and set values to those recommended by security best practices when possible.

OCIO's Response: The Office of the CIO will work to implement these controls to mitigate potential threats and review our domain controller settings to implement security best practices.

17. Other Items

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.3.2.3, Separation of Duties, states, in part:

> *To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical.*
>
> *Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, audit trails and management supervision must be implemented.*

A good internal control plan includes maintaining documentation on the roles of an application, including the access each role provides a user.

Sound business practice includes pursuing and utilizing services committed to and paid for.

- The Department of Labor did not monitor or review the BPS application claims that were filed and adjudicated by the same employee.

- The Department of Labor did not maintain documentation to support the level of access each UIConnect role granted when assigned to users within the application.

- The Department of Natural Resources (DNR) committed to participating in a statewide contract for an Enterprise Content Management (ECM) system in August 2010. DNR and other participating agencies were billed a monthly per user fee by DAS beginning in February 2011. DNR's monthly fee was $3,960 for the 110 users to whom it committed. As of June 30, 2013, DNR had not yet implemented any ECM solutions for its employees to use, despite the $114,840 paid in user fees. Per DAS, DNR committed to ECM for a period of three years via email.

When one employee can both file and adjudicate the same claim, there is an increased risk that inappropriate or fraudulent claims will be processed, resulting in a loss of State funds. Furthermore, without current documentation of application roles and a description of what access the role provides, there is an increased risk inappropriate access will be inadvertently provided to a user. When an agency does not utilize the IT systems it pays for its employees to use, a waste of State funds results.

> We recommend the Department of Labor periodically monitor and review claims that are both filed and adjudicated by the same employee to ensure the accuracy of those claims. We also recommend State agencies maintain documentation of their application roles, including the access each role grants a user within the application to ensure roles are set up properly, and access granted is in line with management's intentions. We recommend DNR dedicate resources to the timely implementation of technology being paid for.

OCIO's Response: The Office of the CIO will work with agencies when requested to address this business need. Additionally, individual agency responses are offered below:

The Department of Labor responded: As far as the same employee filing and adjudicating the same claim, Adjudication requires the review of previous claims and, when necessary, establishing new claims. For example: with the implementation of legislation creating an Alternate Base Period to qualify for benefits, claimants are now able to file a claim, have initial issues adjudicated, only to receive a monetary determination of ineligibility. Because initial issues have already been determined on the ineligible claim, those issues are then re-established and auto-adjudicated (or manually established and adjudicated) by the next claims filer, who is also an adjudicator. In 2012 this was the case on 158 issues resolved by the same employee who filed the claim. Additionally, since 2008 several Nebraskans have qualified for Extended Unemployment Compensation (EUC) benefits. When a UI Claim exhausts, the claimant must file a EUC claim. All applicable adjudicable issues previously adjudicated on the Regular UI claim must be established and resolved on EUC claims as well. Adjudicators, as function of their job and as a point of customer service, have the authority and responsibility to file new claims in this scenario. The UIConnect request for access has been handled by supervisor's email to the Tax Business Analyst and their backup, the Tax Manager. Prior to processing, the request is reviewed to assure it is consistent with access for the job duties and responsibilities of the position. The supervisor is contacted with any questions about the request that would require additional justification. All requests are processed within the UIConnect security tables. The field representative requests are completed with the filing of a ticket in the Clear Quest system to complete the mainframe portion.Tax management will work with Internal Security and IT staff to include UIConnect access request documents within the Access Request Process (ARP) system. The Tax and IT staff will develop detailed documentation for each UIConnect access role. Establishing a crystal report to be reviewed by Internal Security on a monthly basis all claims filed and adjudicated by the same employee. Suspicious transactions in the report will be investigated by Internal Security and fully documented.

The Department of Natural Resources responded: The Department entered into an agreement with the OCIO in August 2010 to lock in a reduced fee structure for its use of the OnBase application. DNR was and continues to be committed to implementing OnBase, and fully expected to be much further along in that process by this point in time. Although delayed in achieving the original plan for fully implementing production ECM workflows, DNR's ongoing development project has thus far yielded work flow designs and preliminary ECM configuration specifications for two processes as well as tested applications to migrate existing electronic records to the ECM database. Three key factors contributed to project delays: 1) for about 12 months, the vendor's software platform lacked specific functionality required in DNR operations; 2) significant time and effort was required to reconcile complex infrastructure differences between the OCIO and DNR technical environments; and 3) senior management was forced to change priorities and divert key IT resources to provide support for immediate and critical issues related to the Republican River Compact lawsuits, compact arbitration proceedings, and related sharing of integrated water management information. Impacts of the above factors have only recently diminished. Key IT resources are now being redirected to the ECM development effort.

* * * * *

Our audit procedures are designed primarily on a test basis and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. Our objective is, however, to use our knowledge of the OCIO and its interaction with other State agencies and administrative departments gained during our work to make comments and suggestions that we hope will be useful to the OCIO.

This communication is intended solely for the information and use of management, the Governor and State Legislature, and others within the Agency and is not intended to be, and should not be, used by anyone other than the specified parties. However, this report is a matter of public record, and its distribution is not limited.

SIGNED ORIGINAL ON FILE

Philip Olsen, CPA, CISA
Audit Manager

SIGNED ORIGINAL ON FILE

Pat Reding, CPA, CFE
Assistant Deputy Auditor