NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

Mike.Foley@apa.ne.gov
P.O. Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
www.auditors.state.ne.us

February 25, 2008

Brenda Decker
Chief Information Officer
Office of the Chief Information Officer
501 S. 14th Street
P.O. Box 95045
Lincoln, NE 68509

Dear Brenda:

The Auditor of Public Accounts (APA) in conjunction with an outside technical consulting firm have completed our examination of information technology (IT) internal control procedures for select applications. These systems support financial reporting and disclosure for the State of Nebraska. Procedures were performed for the fiscal year ending June 30, 2007.

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

The specific confidential details and information were provided separately to agency's management and your office. Following is a high-level overview of the applications included in our testing.

Department of Administrative Services - NIS:

- ***Nebraska Information System (NIS)*** - This application is responsible for processing the financial, human resource, and procurement data business processes for the State of Nebraska. There are extensive interfaces with other state applications.

Department of Health & Human Services (DHHS):

- ***Children Have a Right to Support (CHARTS)*** - CHARTS is used for statewide Child Support Enforcement (CSE). Processes include case initiation, location, establishment, case management, enforcement, financial management, and state/federal reporting. There are extensive interfaces with other state and federal organizations.
- ***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.

- ***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.

Nebraska Department of Education (NDE):

- ***Grants Management System (GMS)*** – This application is used by outside users to apply for grant funds and by NDE to approve and process payments for grant funds. Grant payments made to pre-selected school districts are interfaced with NIS through a separate process.
- ***Quality Employment Solutions through Teams (QUEST)***) – QUEST is utilized by Vocational Rehabilitation staff to track all expenses paid to assist physically and/or mentally disabled persons in locating jobs. It includes aid to complete school, help purchase dress clothes, set up interviews, etc.
- ***Disability Determination System (DDS)*** – The application serves as a customer resource manager and information tracking system for payments to medical practitioners for information they provide to the social security administration pertaining to pending disability claims.

Department of Labor:

- ***Tax Management System (TMS)*** – TMS records daily transactions regarding employer Unemployment Insurance (UI) accounts.
- ***Benefits Payment System (BPS)*** – This application processes payments to eligible claimants and accounts for all overpayment collection activities.

Nebraska Public Employees Retirement System (NPERS):

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

Department of Revenue:

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

Department of Roads:

- ***Project Finance Systems (PFS) –*** Surface transportation projects are managed by PFS.
- ***Maintenance Management System (MMS) –*** MMS manages labor, equipment, materials, maintenance contracts, and indirect costs for routine highway maintenance.
- ***Roads Payment System (RPS) –*** Department of Roads utilizes RPS to process payments to vendors.

State Treasurer:

- ***KidCare*** - The KidCare application supports child support payment processing, including receipt and disbursement for nearly 100,000 child support payments to custodial parents each month.
- ***Wagers*** - The Wagers application maintains information regarding unclaimed property remitted to the State of Nebraska and pays claims for specific property held.

In connection with the examination described above, we noted certain matters involving internal controls over information technology which are presented below for your consideration. These comments and recommendations, which have been discussed with appropriate agencies independently and in detail, are intended to improve the internal controls over information technology.

It should be noted this letter is critical in nature since it contains only our comments and recommendations on the areas noted for improvement.

Comments and Recommendations

1. NIS Technical Support

Assigning appropriately trained staff to the computer processing environments is critical to the successful operation and maintenance of an agency's information systems. Ongoing training helps to ensure staff remains current with new developments related to their job responsibilities. It may also help minimize reliance on key individuals by preparing others to succeed such key individuals and/or to replace them in their absence. Good internal controls include a succession plan in the event key personnel become unavailable to ensure ongoing efficient operation of State business.

The NIS application is a highly customized application which supports multiple financial processes for the State of Nebraska; however, a detailed understanding of the technical and functional application configuration is limited to a very small number of key personnel. A succession plan does not exist in the event key personnel were to become unavailable.

Without a sufficient number of personnel with a detailed understanding of NIS, the level and depth of resources supporting the NIS application may not be able to provide consistent and on-going support over an extended period of time. Specifically, critical systems operation and maintenance activities may not be performed efficiently or effectively when key personnel are unavailable.

> We recommend the Department of Administrative Services (DAS) consider initiating cross training, additional hiring, outsourcing, or other remedial actions.

2. Segregation of Duties

Access to system resources is normally determined by the access privileges granted to a user. In order to retain appropriate segregation of duties, an agency should grant employees adequate system access to perform their jobs, and prevent unauthorized access. Changes in an employee's

role or responsibility may require a change in the access privileges associated with his or her user id.

- Seventy-three State employees with NIS daily processing access had the ability to create and approve their own accounting entries.
- Sixteen out of 23 users with the authority to approve payments in the RPS application also had access to initiate payments and these transactions could go unmonitored.
- Sixty-two employees had the ability to prepare and approve claims within the Department of Labor's BPS application.

Employees with the ability to both prepare and approve accounting transactions in an application increases the risk of unintended or unauthorized transactions being processed. Employees with this access can process financial transactions without anyone else's knowledge or involvement. As a result, unapproved or inaccurate payments could be made.

> We recommend a user's ability to both initiate and approve transactions be eliminated. This access should be segregated so the same user cannot perform both of these functions in an application. If this level of access is necessary to perform job functions, an independent alternate review should occur on a continuous basis to ensure transactions prepared and approved by the same person are appropriate and correct.

3. Developer Access to Production Environment

Access to information resources should be restricted based upon job responsibilities to help enforce proper segregation of duties and reduce the risk of unauthorized system access. Programmers should generally be limited to accessing only the information specifically required to complete their assigned systems development projects, and expressly prohibited from directly accessing production software and data information. Computer operators normally should be permitted to run production jobs; however, should be restricted from accessing the development environment. Access to production program libraries and data information should be logged and periodically reviewed for appropriateness.

- Three application developers at the State Treasurer's office had administrator access to the Windows environment and to the database. Two of these application developers also had administrative access to the Kidcare application.
- Two NIS application developers maintained administrator access to the server environment and the supporting database.
- One Department of Revenue employee had the ability to administer servers housing the GPS, Homestead, and Motor Fuels applications, approve application changes, and promote changes to the production environment.
- All QUEST application programmers at the Department of Education had access to the production environment, could make modifications directly to the production environment, and were responsible for implementing security changes.

Application developers with access to the database and the production environment have the ability to circumvent the standard change control process and implement modifications that may not be consistent with management's intentions.

> Due to the size of the information technology department, developers may need access to the production processing environment. In order to mitigate the risk of moving unintended changes into production, compensating controls should be established. We recommend developers be required to obtain approval prior to moving changes into production. In addition, a review of audit logs should be conducted for changes made to the production environment.

4. Access Commensurate with Job Responsibilities

Users improperly granted the ability to make changes to system security parameters may result in unapproved changes being implemented. Unauthorized modifications to job scheduling software may result in unauthorized, incomplete, or inaccurate processing and excessive maintenance or support to correct processing problems. If such access is not implemented and configured properly, business cycle controls may be ineffective. Additionally, significant information resources may be modified inappropriately, disclosed without authorization, and/or unavailable when needed.

- After evaluating users of the NIS functional areas, we determined 33 of 131 user ids tested had access that was not required for their job responsibilities. The elevated privileges were in the accounts receivable; general ledger; accounts payable; fixed assets; and human resources functions of NIS.
- Department of Roads established a group to control mainframe security access rights for all Department of Roads' personnel. NIS datasets were used to transfer invoice data, general ledger account updates, and voucher data from the RPS application to NIS. However, the mainframe group granted 2,219 employees ALTER access to three NIS datasets tested. ALTER access allows the user to read, change, create, or delete a dataset.
- Nineteen DHHS users were identified with access to sensitive datasets who did not require this access to complete their job responsibilities.
- One DHHS, one Department of Roads, and one Office of the Chief Information Officer (CIO) user had the ability to make security setting changes not required as part of their job responsibilities.
- One Office of the CIO user had UPDATE access to system datasets who did not require it as part of their job responsibility. UPDATE access allows the user to read and make changes to a dataset.
- One of nine NPERS users with Domain Administrator access did not require administrator privileges as part of their job responsibility. In addition, three users with Domain Administrator access on the database server had a password shared among the IT staff.
- Two of six Department of Education staff level users with administrative level access privileges within the GMS application did not require this functionality to complete their job responsibilities.

- Three Department of Labor users had access to the production scheduling functions on the mainframe and did not require this access as part of their job responsibilities.
- The State Treasurer's office had 142 users with administrator privileges on the Wagers application server that were not consistent with their respective job functions. A periodic review of access privileges was not performed.
- Activation codes utilized by Department of Education - GMS users to gain application access were the same for all users and a regular change schedule was not maintained. These activation codes were utilized by administrators at the district level to grant additional access to the application and were the same for each user granted access to the application. The activation codes were not changed unless a request was made by a district administrator. Policies and procedures were not in place to document user access to the GMS application.

Without a proper segregation of duties, programmers or system administrators have the capability to create and approve unauthorized changes if they choose to do so. When an individual has access not required by their job duties, there is an increased risk for the loss of State funds due to error or fraud. There is also a risk that unauthorized transactions or changes could occur. Without periodically changing the activation codes allowing access to an application, there is an increased risk users may gain unauthorized access through the utilization of a single access code.

> We recommend all application owners review a list of their users and verify access levels are accurate. This should be done on a periodic basis to ensure access to the application is commensurate with employees' job responsibilities. We also recommend the application owners eliminate the practice of shared passwords and activation codes.

5. Dataset Access

Typically, entities restrict access to information resources (e.g., programs, data, networks) to enforce desired segregation of duties, facilitate on-line approvals, and help achieve business cycle control objectives. Logical security tools and techniques are used to define such access restrictions, including how and to whom the entity will limit the ability to view, use, or modify significant information resources.

- Two Department of Labor application developers had access to production datasets for the Tax Management System application.
- DHHS application developers maintained access to production datasets for CHARTS, MMIS, and NFOCUS applications. One to seven application developers for each application had ALTER access to production datasets.

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

of a systematic log of changes made to production, management does not have an effective method for auditing change management practices.

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

6. New and Terminated User Access

Changes in an employee's role or responsibility may require a change in the access privileges associated with a user id. These changes should be performed immediately upon the change of the employee's status. A specific, high-risk example of this is the loss or termination of an employee. Former employee system access should be immediately revoked, especially if remote access facilities exist. Periodic inspections, based on independent information that could be obtained from the human resources department, should ordinarily be performed by management to ensure necessary changes have been made.

- The Department of Education utilized a portal for their GMS application. There was no process in place to ensure district administrator accounts were removed in a timely manner in the event of user termination. Also, passwords could be utilized for an unlimited amount of time with no change requirement.
- Three of nine terminated user ids tested at the Department of Labor had not been deleted or disabled from the BPS application within a timely manner. One of nine new BPS user accounts did not have a completed new user access form on file to formally approve the user's respective access rights. In addition, a periodic review of user access to the BPS application was not completed.
- The Department of Revenue had no formalized user administration process to grant access to Windows applications.
- Four of nine State Treasurer terminated user ids had not been deleted or disabled from the system.

The identification and authentication of users serves to validate the people who use computer systems. Inadequate approval of access or a lapse in removing access may lead to financial loss, operational damage through unintentional access, or deliberate unauthorized access. Access to networks and applications not approved, terminated timely, or configured appropriately creates the opportunity for unauthorized processing of transactions, and access to critical system settings.

> We recommend application owners review user access on a periodic basis to ensure access is appropriate. Additionally, a formalized process to grant access to applications should be established and followed. Terminated users access should immediately be revoked or removed.

7. Shared IDs

Sharing of privileged ids poses a threat to security because over time these user ids and passwords may become known to individuals not intended to have this level of access. The individual user ids should be used to validate their use of the computer systems. A user id distinguishes one user from another, and establishes accountability for system-based actions.

- DHHS utilized four shared ids with Domain Administrator privileges. Domain Administrators had the ability to make system and security changes.

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 DHHS eliminate all shared ids to ensure individuals have a unique id to make users accountable for transactions on computer systems.

8. Password Security

On April 20, 2007 the Department of Environmental Quality (DEQ) sent a payment of approximately $1.8 million to an incorrect vendor. On May 4, 2007 the recipient contacted the Department of Administrative Services about the receipt of the $1.8 million. The Department of Administrative Services reversed the transaction on May 8, 2007 and sent the payment to the correct vendor.

In discussion with DEQ, it was determined the internal controls in place were circumvented and an employee's user id was used in his absence to process the payment on NIS. The DEQ Authorized Agent locked out the individual's account by entering the password three times incorrectly, and then requested a new password be issued. When the password was re-issued, it was sent to the DEQ Authorized Agent, who then processed the incorrect payment.

In some instances, a few key personnel have the ability through elevated access to circumvent internal controls. Individuals with the ability to circumvent established internal controls increases the risk for errors, fraud, and/or the misappropriation of State funds.

> We recommend DEQ establish policies to ensure payments to vendors are properly reviewed before being posted. We also recommend staff be educated about the importance of internal controls, and consider training additional staff to perform duties as a backup.

9. Password Complexity

User access is generally controlled through passwords. Passwords should be changed periodically and a complexity of the length or types of passwords should be maintained.

- Password complexity was not enabled for the NIS database environment.

- Servers at the Department of Revenue did not have a minimum password age or minimum password length requirement.

The utilization of short passwords increases a systems susceptibility to hacking. Strong and complex password settings reduce the risk of an unauthorized user gaining access to confidential information and key financial data.

> We recommend password complexity requirements be implemented.

10. Physical Security and Environmental Controls

An entity's information resources include computer hardware, peripheral devices, data storage media, and information systems documentation. Physical access to such resources makes it possible for the user to view, use, damage, or misappropriate these resources. Accordingly, such access should be restricted to authorized personnel. Damage to information resources, including computer hardware, data storage media, and information systems documentation, can result from a variety of causes, including heat, smoke, fire, humidity, flooding, earthquakes, and electrical disruption. Typical countermeasures to address these threats include alarm systems (for heat, smoke, fire, and/or moisture), fire suppression equipment, air conditioners, raised floors, air filters, uninterruptible power supplies, batteries, generators, and earthquake-resistant flooring and construction. The nature and extent of countermeasures should be based on management's periodic assessment of the business impact of each potential threat.

- There were no fire or water detection tools located within the State Treasurer's datacenter. The security camera used to monitor the datacenter was disabled. Security access to the datacenter was controlled with a Personal Identification Number (PIN) number shared by employees. The PIN number was not changed on a periodic basis.
- Forty-nine of 111 individuals with access to a DHHS server room did not require the access as part of their job responsibility.

Exposure to heat and water can damage information resources, including computer hardware, data storage media, and information systems documentation. The lack of monitoring access to the datacenter as well as sharing the PIN number can lead to key financial information being more susceptible to theft, damage, and misuse.

> We recommend countermeasures, like an alarm system and fire suppression equipment, to address threats of heat, smoke, fire, and moisture. We recommend employees be given their own unique PIN number to access the datacenter in order to establish accountability. We also recommend only authorized personnel have access to information resources and access to these resources be reviewed on a periodic basis to ensure only authorized individuals have access.

11. Standardized Change Management Process

A formal methodology should be in place to guide the development of applications and systems. Changes to existing applications and systems should undergo an evaluation, authorization, and implementation procedure to ensure they have the intended effect and minimize user disruption. Insufficient evaluation, planning, and testing of modifications could cause unexpected disruptions to an Agency. These disruptions could negatively impact the completeness and accuracy of data or could result in implementation of system changes that are unable to meet the entity's information processing needs.

- The Department of Roads had not implemented a standard and consistent change control process for database, application, and network modifications. The Department of Roads relied on informal methods of communicating change requests and requirements. Specifically, 7 of 15 application/database changes tested did not have supporting change documentation; including documented requests, testing documentation, or management approval to implement changes into production.
- The State Treasurer did not have a standard process to implement and track Wagers application changes. The Wagers application did not utilize a separate testing environment to test modifications prior to being implemented into production. Documentation for testing of the Wagers application changes was not maintained. There was not adequate supporting documentation for 5 of 15 KidCare application changes tested. One of the 15 changes tested did not have a completed cutover sheet which contains a brief summary of changes made and provides documentation of management review.
- The Department of Revenue had not implemented a standard and consistent change control process for system software modifications. Test documentation for the Motor Fuels application modification was not retained to support the change functioned according to management's intentions.
- NPERS did not test 1 of 15 sampled changes to the PIONEER application before the change was moved into production.
- The Department of Education did not have a formal documentation flow and retention policy to document the initial change request, management's subsequent approval, testing, and review of the change after implementation of the proposed change for changes related to the GMS and systems software.

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

We recommend a standardized change management process be developed and implemented for application and systems changes. The process should include documented change requests, approvals, testing procedures, and approval to implement the change into production. In addition, all modifications to application systems should be tested in an environment separate from the production processing environment.

12. System Monitoring

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

- System events were not monitored by the NIS support staff, NPERS, or the State Treasurer's office to verify they were operating according to management's expectations.
- The Department of Roads was logging Windows operating system event logs and security violation reports for invalid logons to the Windows network, but were not periodically reviewing these logs.
- The Department of Revenue did not monitor security violation reports for invalid logons to the network to confirm access was obtained according to management's expectations.
- The Department of Education did not monitor processing performed on the GMS servers. Exceptions in processing were not logged or reviewed, and exceptions were not brought to management's attention.

Without monitoring and reviewing data logs to ensure processing occurred successfully, there is an increased risk unauthorized, incomplete, or inaccurate processing will go undetected. Without monitoring security violation reports unauthorized users could access sensitive financial data on the network and financial applications without being detected.

> We recommend a monthly review of critical security events for unauthorized access and inappropriate changes be conducted.

13. Reconciliation of Disbursements/Receipts

Good internal control requires a plan of organization, procedures, and records designed to safeguard assets and provide reliable financial information. Without a timely and complete reconciliation of records, there is an increased risk for fraud and errors to occur and remain undetected.

- After review of five reconciliations sampled for the Department of Labor's BPS application, two did not appear to be adequately performed to ensure all cleared checks were properly recorded in the BPS application.
- One of 25 claims processed and paid by the State Treasurer did not have documentation on file for the payment of unclaimed property. Proof of ownership must be obtained before payment information is sent to NIS and claims are paid.
- The Department of Education did not complete a formal reconciliation for the GMS to NIS batch payments. In addition, the application did not have appropriate edit checks in place to prevent a user from re-submitting a payment batch.

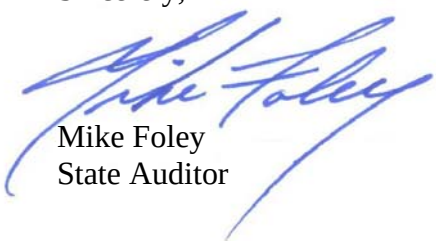
The reconciliation process may identify either reconciling items or discrepancies requiring adjustment. Recording checks disbursed without reconciliation to the bank balance could result in transactions not being accurately or completely recorded. Poorly designed reconciliation processes may not detect human errors or financial reporting balancing issues.

Without confirming proof of ownership, property may be disbursed to unintended individuals.

We recommend a formal reconciliation process be implemented to ensure all transactions are accounted for and properly recorded. We also recommend claims to unclaimed property be supported by proofs of ownership. Automated controls could be established to prevent claims without proper documentation from processing.

We appreciate and thank all employees involved in the Information Technology examination for their cooperation and courtesy extended to our staff during the engagement.

Sincerely,



Mike Foley
State Auditor