NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Charlie Janssen
State Auditor

Charlie.Janssen@nebraska.gov
PO Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
www.auditors.nebraska.gov

January 30, 2017

Courtney Phillips, Chief Executive Officer
Nebraska Department of Health and Human Services
301 Centennial Mall South, 3rd Floor
Lincoln, Nebraska 68509

Dear Ms. Phillips:

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the State of Nebraska (State) as of and for the year ended June 30, 2016, 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, we have issued our report thereon dated December 15, 2016. 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 that are appropriate in the circumstances for the purpose of expressing our opinions on the 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 activities of the Nebraska Department of Health and Human Services (Agency) 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 Agency'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. However, as discussed below, we identified certain deficiencies in the Agency's internal control that we consider to be significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. We did not identify any deficiencies in internal control that we consider to be material weaknesses.

A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider Comment Number 1 (Material Adjustments), Comment Number 2 (Medicare Part D), Comment Number 3 (Overpayment Mailbox), Comment Number 4 (Overpayments), and Comment Number 5 (External MMIS User Access) to be significant deficiencies.

Those comments will also be reported in the State of Nebraska's Statewide Single Audit Report Schedule of Findings and Questioned Costs.

In addition, we noted other matters involving internal control and its operation that we have reported to management of the Agency, pursuant to AICPA Auditing Standards AU-C Section 265.A17, in separate early communication letters dated September 7, 2016, and September 28, 2016.

Draft copies of this letter were furnished to the Agency 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 they will be verified in the next audit.

The following are our comments and recommendations for the year ended June 30, 2016.

1. Material Adjustments

The Department of Administrative Services, State Accounting Division (DAS), prepares the State of Nebraska Comprehensive Annual Financial Report (CAFR) and requires all State agencies to determine and report accurate amounts for financial reporting.

The Agency indicated in its response to the Summary Schedule of Prior Audit Findings that its corrective action plan was complete regarding errors in accrual information. However, throughout testing, we noted the following items were not accurately reported to DAS:

- The Agency understated short-term payables by $2,051,744 related to the Indirect Medical Education (IME) and Direct Medical Education (DME) payments owed at June 30, 2016, but not yet paid to providers. When compiling the accrual response form, prior year figures were used instead of developing reasonable estimates based on historical and available data. The Auditor of Public Account's (APA's) proposed adjustment was made by DAS to correct the error. An additional amount of $871,858 of IME and DME long-term payables was determined to be understated for similar issues; no adjustment was proposed or made for this amount.

- The State Ward payable was overstated by $1,404,773. The amount was coded within the State accounting system as a payable at June 30, 2016, and the Agency included the amount on the accrual response form, resulting in it being counted twice. The APA's proposed adjustment was made by DAS to correct the error.

- The Medicaid, State Disability, and Children's Health Insurance Program (CHIP) payable was overstated by $2,600,000, as an adjustment was counted twice. The APA's proposed adjustment was made by DAS to correct the error.

- The Third Party Liability (TPL) receivable is for balances due from legal obligations of third parties (i.e., individuals, insurers, program, etc.). The Agency calculated the receivable by averaging total amounts recovered over the past eight years, representing the amount expected to be recovered during an entire fiscal year. The Agency estimated that only recoveries made within the first 45 days of the following fiscal year would have been submitted for collection prior to fiscal year end and considered receivable at June 30, 2016. Using this criteria as a guide, the APA calculated an overstatement of the TPL receivable to be $6,949,955. The APA's proposed adjustment was made by DAS to correct the error.

- The Medicaid Drug Rebate (MDR) program accounts receivable was overstated by $7,612,893, due to rebate checks on hand at the Agency that had not been recorded in the State's accounting system or the MDR system. The APA's proposed adjustment was made by DAS to correct the error. An additional amount of $264,418 was determined to be overstated due to mathematical errors and figures not updated from the previous year when calculating the receivable balance; no adjustment was proposed or made for this amount.

- The patient and county billings receivable was overstated by $233,240, as account balances approved for write-off by the State Claims Board were not removed. An additional amount of $19,334 was determined to be overstated, as 5 of 25 patient balances tested were not pursued by the Agency for collection or written-off in a timely manner. No adjustments were proposed or made for these immaterial amounts. Four of those five balances were inaccurately reported as receivables.

- A $3,031,549 journal entry was made in fiscal year 2016 to correct a duplicate entry made in fiscal year 2015. The entry was not properly recorded as a prior period adjustment, resulting in an overstatement of current year Federal fund expenditures and an understatement of General fund expenditures. DAS passed on the APA's proposed adjustment.

- On a quarterly basis, costs associated with printing and producing occupational licenses are allocated to various programs. The entry used to allocate expenditures incorrectly used transfer in/out account codes, which resulted in revenues and expenditures being overstated by $789,562. The APA's proposed adjustment was made by DAS to correct the error.

- Cash was overstated by $1,298,169, as a disbursement from the State Ward Child Support account on June 3, 2016, was not included in fiscal year 2016 bank activity. The APA's proposed adjustment was made by DAS to correct the error.

A similar finding was noted during the previous audit.

Title 2 CFR part 200.511(a) (January 2016), requires the auditee to prepare a summary schedule of prior audit findings. Per subsection (b)(2) of that same regulation, "When audit findings were not corrected or were only partially corrected, the summary schedule must describe the reasons for the finding's recurrence and planned corrective action, and any partial corrective action taken."

A good internal control plan requires agencies to have procedures for the reporting of accurate and complete financial information to DAS.

Without adequate processes and procedures in place to ensure the accuracy of financial reporting, there is a greater risk material misstatements may occur and remain undetected.

> We recommend the Agency implement procedures to ensure information is complete and accurate. The Agency should also have adequate procedures in place for a secondary review to verify the information is supported, reasonable, and accurate.

Agency Response: The Agency agrees with the condition reported.

Corrective Action Plan: Since the issuance of the 2013 Single Audit, the Agency has implemented several improvements to the CAFR accrual reporting process that has resulted in fewer errors in recent Single Audits. Financial Services staff in cooperation with Internal Audit hosts an annual CAFR kick-off meeting with all staff involved in the reporting process and includes DAS Accounting in these meetings. This meeting outlines the internal reporting process, documentation expectations, prior year audit findings and deadlines. Documentation for each accrual item is then collected and compiled by Financial Services based on a pre-defined and communicated deadline for an initial review and then is subsequently reviewed by Internal Audit staff.

The IME/DME accrual calculation was new to the 2015 and 2016 CAFR and had no adjustments noted during the 2015 CAFR. The audit adjustment for 2016 was due to the fact that documented procedures, while adhered to, relied on using prior year long-term payable calculations as a basis for current year short-term payable calculations. Procedures will be modified to include an annual recalculation of estimates.

The adjustment for TPL was due to the fact that the Agency modified its procedures for calculating this particular receivable. The Agency proposed a change in reporting to improve accuracy which was agreed to by DAS. It was discovered during the audit that the Health portion of this receivable was overstated due to the fact that Health claims receivable turnover is much higher than the casualty and should have been limited to those only claims submitted within 45 days prior to the end of the fiscal year.

The majority of the MDR receivable overstatement was due to the rebate checks on hand but not yet processed. Currently all of these checks have now been processed and the Agency has revised internal procedures to ensure timely processing of these rebate checks.

The cash overstatement was due to a transfer of funds from an external bank account into the State's banking system while working with the State Treasurer's Office to address collateralization issues. This amount was not removed from the accrual response form to DAS.

2. Medicare Part D

The Lincoln Regional Center (LRC) claims for Medicare Part D (Medicare Prescription Drug Coverage) have not been billed to the responsible parties since November 2013. According to the Agency, there were balances totaling $2,261,151, as of June 30, 2016, which are anticipated to be unrecoverable due to the passing of the maximum allowable time to recover lost revenues.

According to the Agency, various issues with the vendor's system and contract procurement process had prevented the Agency from pursuing reimbursement for Medicare Part D since November 2013. The APA had a finding regarding this issue in the prior audit.

A similar finding was noted during the previous audit.

Sound accounting practices and good internal controls require policies and procedures to pursue and resolve issues related to receivable balances.

When receivables are not billed for an extended amount of time, there is an increased risk for the loss of State funds due to the inability of DHHS to bill for reimbursement based on time restrictions.

> We recommend the Agency work to resolve their billing issues, so Medicare Part D claims can be submitted and reimbursed to the State.

Agency Response: The Agency agrees with the condition reported.

Corrective Action Plan: As indicated during the review, Lincoln Regional Center (LRC) is actively working to resolve the contractual and software problems that have impeded billing responsible parties for Medicaid Part D claims since 2013. While software issues and contracts with intermediaries were being resolved, paper billings were not permissible by Medicare. Since April, 2016, Agency Legal and LRC staff have worked with the Center for Medicare Services (CMS) Intermediaries to reinstate the required contracts. At the same time, the vendor has worked to resolve software issues impeding the billing process. As of this response, ongoing billing is occurring with two intermediaries, a third intermediary contract has been signed by the Agency and is waiting the intermediary signature, and the remaining intermediary contracts are in process. Active billing for Medicare Part D claims is being conducted with the intermediaries as contracts are finalized and subsequently allowed. Recovery of prior billings is limited to sixty days.

3. Overpayment Mailbox

On November 30, 2011, the Agency set up the Overpayment Mailbox (Mailbox) for eligibility overpayments. Previously, Social Service Workers (SSWs) would set up overpayments and underpayments in the Nebraska Family Online Client User System (NFOCUS) as they discovered them. Eligibility overpayments were referred via email to the Mailbox to be worked by an Overpayment (OP) Unit team.

In the prior audit, we noted 12,525 referrals were unworked. The situation has not changed significantly – the figure as of June 30, 2016, was 11,580 unworked referrals. However, the Agency also had 5,687 unworked referrals labeled as "Non Pursuable," of which 5,413 were Supplemental Nutrition Assistance Program (SNAP) errors made by the Agency. This brings the total of unworked referrals to 17,267.

The Agency indicated the referrals were not pursuable because they were over 12 months old, which is in accordance with the Agency's regulations at 469 NAC 3-007.03B2 and 475 NAC 4-007.01A. Per 475 NAC 4-007.01A, "Overpayments must be established against households who were issued benefits they were not entitled to receive due to an AE [Administrative Error] for no more than 12 months before the month of initial discovery." However, this State regulation conflicts with 7 CFR § 273.18(c)(1), which requires the agency to "calculate a claim back to at least twelve months prior to when you became aware of the overpayment." (Emphasis added.)

Even if the Federal regulations did not exist, common sense and good internal control would suggest the original intent of the State regulations was not to allow the Agency to sit on overpayment referrals until they are over 12 months old, and then discard them.

We also noted that using the Outlook email account increases the risk that referrals will be inappropriately deleted.

SNAP regulation 7 CFR § 273.18(d)(1) (January 1, 2016) requires the State to "establish a claim before the last day of the quarter following the quarter in which the overpayment or trafficking incident was discovered." The Agency follows this timeframe for all programs. A good internal control plan requires procedures to be in place to ensure overpayments are established in NFOCUS in a timely manner.

Without adequate controls and resources to work suspected overpayments, timeframes set by Federal regulations may not be met. Overpayments not worked timely have a lesser chance of collection. Overpayments not worked at all will have no chance of collection. There is less incentive for the Agency to pursue collection on SNAP AE overpayments, as the Federal government requires all of those collections to be returned in their entirety to the Federal government. However, those overpayments increase the taxpayer burden at the Federal level, and the Agency should actively pursue those receivables. Considering the number of referrals not worked, there are potentially millions of dollars in overpayments that the Agency has not attempted to recover.

> We recommend the Agency implement procedures and devote adequate resources to investigating and establishing NFOCUS receivables. If the Agency continues to use the Mailbox for eligibility overpayments, care should be taken to ensure all emails are properly tracked, monitored, and maintained. We recommend the Agency define the date of discovery as the date the regular SSW first becomes aware of a potential overpayment. The Agency should comply with Federal regulations. We also recommend the Agency implement procedures to reduce the number of SNAP AE overpayments.

Agency Response: The Agency agrees with the condition reported.

Corrective Action Plan: The Agency created an overpayment team with primary responsibility for working overpayment referrals and secondary responsibility as backup for AccessNebraska. Access to the overpayment mailbox has been limited to only staff with a business requirement. Currently referrals are received at a rate of 150 per week and current procedures and resources allow for 50 referrals per week to be completed.

The Agency will begin a more in-depth review of the current referral process as well as the steps and procedures for reviewing and establishing an overpayment for operational efficiencies. Additionally, the Agency is reviewing the feasibility of utilizing an Access database to store referrals as a replacement of the Outlook Mailbox for enhanced controls.

The Agency will modify procedures and communicate to relevant staff of the federal timeline requirements for establishing overpayments.

4. Overpayments

During testing of nine accounts receivable from NFOCUS, we noted various errors, as described below.

Receivables Not Set Up Timely

Four of six accounts receivable tested were set up after the calendar quarter, following the date of discovery. The receivables were set up 156, 152, 125, and 69 days late.

Per 7 CFR § 273.18(d)(1) (January 1, 2016), a State must "establish a claim before the last day of the quarter following the quarter in which the overpayment of trafficking incident was discovered."

Collection Policy Not Followed

The Agency's own Collection Policy was not followed for three of nine receivable accounts tested. One receivable balance was suspended because the Agency was unable to locate the provider. When a receivable is suspended, no collections efforts are performed. The provider's address was later updated when the provider applied for, and received assistance for, other NFOCUS programs; however, the account remained suspended. For the second account tested, the procedure for accounts 90 days overdue was not followed, as a director letter was not sent to the provider. For the third account, the first billing statement was sent two months late, and the director and legal letters were not sent.

Good internal control requires the Agency's Collection Policy and payment agreements to be followed. The Agency's Collection Policy states, in part, the following:

> *(2) DHHS will send regular billing statements for all accounts receivable, except when prohibited by law.*
>
> *(3) [F]or accounts which are 90 days overdue, unless suitable arrangements have been made for payment:*
>
> *a. DHHS will send the Debtor a letter, signed by the appropriate Director, requesting payment.*
>
> *b. If no response is received within 30 days of the initial letter, DHHS will send the Debtor a second letter, signed by a DHHS Legal and Regulatory Services (LRS) attorney, again requesting payment . . . .*

c. *If no response is received within 30 days of the second letter, DHHS will take….action, based on the dollar value of the account.*

(6) Except in situations where collection efforts are required by law, DHHS will suspend collection efforts, with the exception of monthly billing statements, during any period that the Debtor is receiving state or federal needs-based assistance, whether or not the statute of limitations may expire prior to the termination of the needs-based assistance.

Missed Recoupments

For two accounts receivable tested, the providers were receiving payments in NFOCUS. As such, a portion of the provider payments should have been recouped and applied towards the receivable balances. For one account, potential recoupments totaling $235 were missed during the fiscal year. For the other account, five months of recoupments, totaling $50, were missed.

Per Title 475 NAC 4-007.02A, related to SNAP, "Collection on Accounts Receivable will be done through recoupment from the household's benefit or by other collection actions."

Per Title 392 NAC 5-005, related to Child Care, "If the provider does not appeal or contact the Department to work out a repayment agreement, the overpayment will be recouped from future billings for the same or different children, or from another service."

Receivable Mishandled

A beginning receivable balance of $258 was overstated by $109. In an attempt to correct the balance, the Agency created a second receivable balance for the correct amount of $149; however, the incorrect balance of $258 was not removed.

A similar finding was noted during the previous audit.

A good internal control plan and sound business practices require procedures to ensure receivable balances are accurate.

Inadequate controls and procedures result in fewer collections of Federal and State funds that could be used to reduce the taxpayer burden.

> We recommend the Agency implement controls and procedures to ensure policies are followed. The Agency should review its collection policy and consider automating more collection processes in NFOCUS.

Agency Response: The Agency agrees with the condition reported.

Corrective Action Plan: The Agency implemented new standard operating procedures and a new system using Microsoft SharePoint to ensure that all receivables for provider overpayments are set up timely, improve monitoring and reporting, and reduce the error risk. The new procedures include random quality verification to self-audit for accuracy as well as a weekly review of newly activated clients and providers who have an open account receivable.

A revised Collection Policy has been drafted and is currently in management review which includes several internal procedural changes to ensure adherence to policy requirements.

5. External MMIS User Access

The Medicaid Management Information System (MMIS) supports the operations of the Medicaid Program. 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.

In our review of access to MMIS, we noted that 402 of 919 external users tested at 9 external entities were no longer current and active employees of the external entity or no longer needed access to MMIS. For one other external entity, we were not able to verify that the 47 users were current and active employees of the external entity and required access to MMIS.

The APA requested contact information for 10 of 836 external entities for MMIS to determine if users were still active employees and needed access to perform their job duties. The entities selected and the results of this inquiry were as follows:

MMIS External Entities			
Entity	**Exceptions**	**Total Users**	**% Not Needing Access**
Aegis Sciences Corporation	8	20	40.0%
AmeriHealth Nebraska Inc.	219	364	60.2%
Boys Town	0	121	0.0%
Fallbrook Family Health Center	13	21	61.9%
Kohls Pharmacy and Homecare	43	82	52.4%
Magellan	18	52	34.6%
NE Methodist Health System	55	148	37.2%
One World Community Health Center	37	93	39.8%
Thayer County Health Services	9	18	50.0%
Total	**402**	**919**	**43.7%**

The APA also selected Children's Hospital Colorado but was unable to verify that the users were still active employees who needed MMIS access to perform their job duties.

A similar finding was noted during the previous audit.

The Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.7.2, User Account Management, states the following, in relevant part:

> *A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (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.*

A good internal control plan requires terminated users' access to be removed timely.

The external entities did not inform the Agency timely when employees were terminated. The Agency performs a review of external users' access only once a year.

Failure to terminate former user access to networks and applications creates the opportunity for unauthorized access to Federally protected State data.

> We recommend the Agency improve procedures by performing more routine reviews of external users' access in order to ensure unauthorized access is removed in a timely manner. We also recommend the Agency periodically inform external entities of the importance of notifying the Agency to remove employee access upon termination.

Agency Response: The Agency agrees with the condition reported.

Corrective Action Plan: Recently the EDI Help Desk has coordinated with MMIS to enhance several processes as well as identify and remove users that no longer require access. These enhancements decreased the amount of time to process enrollments for external users by moving the external user data from an Excel spreadsheet to an Access database as well as a system change implemented in October 2016 for the user account management process.

EDI has improved the timeframe for disenrollment of External MMIS Users without a need for access by streamlining the process for external user verification and implementing a process for provider outreach. Additionally the Agency implemented improved standards to enhance the process of monitoring provider response to verification outreach. These processes include requiring a detailed response regarding all enrolled individuals, and dis-enrolling non-responsive providers within a designated time period. When verification is requested, providers are reminded of the importance of notifying the Agency to remove access to External MMIS Users upon their termination. The notification highlights the requirement of External Users to notify the EDI Help Desk of any staffing changes or separations of individuals that have External MMIS User Access. These improvements have enabled the EDI Help Desk to successfully complete verification of 78% of all External Access Users over the course of 2016. The EDI Help Desk has also shortened the designated time period allotted to providers to reply to verification requests.

6. Unauthorized Accounts Utilizing State's Federal Tax Identification Number (FTIN)

During the prior year audit, the APA identified a bank account that was using the State's FTIN; however, the account was not authorized by the State Treasurer to do so. The account was still using the State's FTIN and had not been authorized by the State Treasurer as of June 30, 2016.

Agency	Bank Name	Account Name or Owner	Account Number	Balance at 6/30/2015
DHHS	Pinnacle Bank	DHHS – Bridges Program Residents	XXX252	$ 377.00

A similar finding was noted in the previous audit.

Neb. Rev. Stat. § 77-2301(1) (Reissue 2009) requires the following:

> *The State Treasurer shall deposit, and at all times keep on deposit for safekeeping, in the state or national banks, or some of them doing business in this state and of approved standing and responsibility, the amount of money in his or her hands belonging to the several current funds in the state treasury. Any bank may apply for the privilege of keeping on deposit such funds or some part thereof.*

Neb. Rev. Stat. § 77-2309 (Reissue 2009) requires the following:

> *It is made the duty of the State Treasurer to use all reasonable and proper means to secure to the state the best terms for the depositing of the money belonging to the state, consistent with the safekeeping and prompt payment of the funds of the state when demanded.*

Neb. Rev. Stat. § 77-2398(1) (Cum. Supp. 2016) requires public funds in financial institutions to be secured by the appropriate amount of pledged collateral. That statute provides the following, in relevant part:

> *As an alternative to the requirements to secure the deposit of public money or public funds in excess of the amount insured or guaranteed by the Federal Deposit Insurance Corporation pursuant to sections 77-2389 and 77-2394, a bank, capital stock financial institution, or qualifying mutual financial institution designated as a public depositary may secure the deposits of one or more governmental units by providing a deposit guaranty bond or by depositing, pledging, or granting a security interest in a single pool of securities to secure the repayment of all public money or public funds deposited in the bank, capital stock financial institution, or qualifying mutual financial institution by such governmental units and not otherwise secured pursuant to law, if at all times the total value of the deposit guaranty bond is at least equal to the amount on deposit which is in excess of the amount so insured or guaranteed or the aggregate market value of the pool of securities so deposited, pledged, or in which a security interest is granted is at least equal to one hundred five percent of the amount on deposit which is in excess of the amount so insured or guaranteed.*

A good internal control plan requires a periodic review by the State Treasurer of those accounts under the State's FTIN to ensure that all such accounts are properly authorized and secured by the appropriate amount of pledged collateral.

When bank accounts are opened and operated under the State's FTIN without the authorization of the State Treasurer, there is an increased risk of loss or misuse of State funds and concerns regarding insufficient pledged collateral to secure the amount of public funds in excess of FDIC coverage.

> We recommend the Agency remove the State's FTIN from any unauthorized bank accounts. We also recommend the Agency work with the State Treasurer to ensure all bank accounts using the State's FTIN are operated under the control or approval of the State Treasurer.

Agency Response: See response to comment number 7.

7. Agency Accounts Not Under Control of State Treasurer

The APA found during the prior year audit that the Agency was maintaining bank accounts without the prior approval of the State Treasurer to do so. As of June 30, 2016, the Agency still did not have the State Treasurer's approval for these bank accounts. According to State law, one of the duties of the State Treasurer is to establish banking relationships for the State of Nebraska; therefore, any bank account used by a State agency should be authorized and approved by the State Treasurer. Below is a summary of the bank accounts identified by the APA as being maintained without the State Treasurer's approval, as of June 30, 2016.

a) DHHS Emergency/Petty Cash Accounts

Thirteen petty cash bank accounts held by the Agency were still deposited into separate bank accounts without the prior approval of the State Treasurer. The lack of prior approval was noted at June 30, 2015, and the following petty cash accounts still did not have State Treasurer approval as of June 30, 2016.

	Agency	Name	Account Name or Owner	Account Number	Balance at 6/30/2015	APA Notes
1	DHHS	First National Bank of Omaha	DHHS – Eastern Nebraska Veterans' Home	XXX383	$ 2,528.08	Emergency cash account.
2	DHHS	Pinnacle Bank	DHHS – Accounting Unit	XXX703	$ 1,283.20	Petty cash for legal fees for legal unit.
3	DHHS	Pinnacle Bank	DHHS – Bureau of Vital Statistics	XXX633	$ 963.50	Petty cash account.
4	DHHS	Pinnacle Bank	DHHS – Beatrice State Developmental Center – Emergency Cash	XXX260	$ 1,477.79	Account for resident activities that include staff admissions, behavior management programs, and change funds for Carstens Café.
5	DHHS	Pinnacle Bank	DHHS	XXX038	$ 1,901.72	Petty cash for legal services.
6	DHHS	York State Bank	DHHS – Youth Rehabilitation and Treatment Center	XXX094	$ 521.50	Petty cash fund.
7	DHHS	U.S. Bank	DHHS – Child Support Enforcement	XXX348	$ 2,038.68	Petty cash for legal services.
8	DHHS	U.S. Bank	DHHS – Child Support Enforcement (CSE) – Petty Cash	XXX313	$ 2,325.98	Petty cash account for payment of sheriff's fees, CSE complaints, contempt's, and modifications.
9	DHHS	U.S. Bank	DHHS – Norfolk Veterans' Home	XXX524	$ 1,548.34	Emergency cash – cash registers account.
10	DHHS	U.S. Bank	DHHS – Western Nebraska Veterans' Home	XXX479	$ 1,705.70	Emergency cash fund.
11	DHHS	Wells Fargo	DHHS – Hastings Regional Center	XXX153	$ 2,239.00	Emergency cash fund.
12	DHHS	Wells Fargo	DHHS – Veterans' Home	XXX523	$ 1,901.50	Emergency cash account.
13	DHHS	Wells Fargo	DHHS – Youth Rehabilitation and Treatment Center	XXX011	$ 1,465.00	Emergency petty cash fund.
			Total Balances at June 30, 2015		**$ 21,899.99**	

Neb. Rev. Stat. § 81-104.01 (Reissue 2014) allows an agency to have a petty cash fund with the approval of the Department of Administrative Services and the State Auditor.

However, per the State Accounting Manual (1/2/15), General Policies #24, Petty Cash, "Petty cash funds should NOT be placed in checking accounts without specific approval from State Accounting and State Treasurer."

Additionally, in Op. Att'y Gen. No 15-010 (Aug. 10, 2015), the Attorney General has stated the following:

> *The State Treasurer is charged with the duty of establishing the banking relationship for the State of Nebraska and its agencies. This is a statutory duty that cannot be delegated and is one of the "core functions" of the Nebraska State Treasurer.*

In that same opinion, the Attorney General concluded as follows:

> *A state agency is not permitted to contract for its own banking relationship; all such relationships are established through the State Treasurer.*

Allowing bank accounts to be opened and operated under the State's FTIN without the authorization of the State Treasurer may result in loss or misuse of State funds or give rise to concerns regarding insufficient pledged collateral to secure the amount of public funds in excess of FDIC coverage.

> We recommend the Agency work with the State Treasurer to ensure all State bank accounts are properly authorized. All bank accounts using the State's FTIN should be operated under the control or approval of the State Treasurer.

b) DHHS Other Bank Accounts

In addition to the Agency petty cash accounts, the Agency maintains a number of other bank accounts under the State's FTIN that do not appear to have been established or approved by the State Treasurer.

- The Agency utilizes four bank accounts for the Veterans' Home member trust funds that use the State's FTIN that do not appear to have been established or approved by the State Treasurer, as of June 30, 2015, and were still not approved by the State Treasurer as of June 30, 2016.

Bank Name	Account Name or Owner	Account Number	Balance at 6/30/2015
Five Points Bank	DHHS – Grand Island Veterans' Home – Member Trust Fund	XXX963	$ 327,358.47
First National Bank of Omaha	DHHS – Eastern Nebraska Veterans' Home	XXX396	$ 102,082.34
U.S. Bank	DHHS – Department of Public Institutions (Western Nebraska Veterans' Homes)	XXX695	$ 21,851.24
U.S. Bank	DHHS – Veterans' Home	XXX607	$ 19,545.28
	Total Balances at June 30, 2015		**$ 470,837.33**

- The Agency maintains two bank accounts for regulation purposes involving complaints against healthcare professionals and welfare fraud; however, these accounts were not reported by the Agency as accounts currently under its control or oversight as of June 30, 2015. These two bank accounts use the State's FTIN but do not appear to have been established or approved by the State Treasurer, as of June 30, 2015, and were still not approved by the State Treasurer as of June 30, 2016.

Bank Name	Account Name or Owner	Account Number	Balance at 6/30/2015
Nebraska State Employees Credit Union	DHHS – Regulation	XXX374	$ 174.72
Nebraska State Employees Credit Union	DHHS – Regulation	XXX630	$ 31.52
Total Balances at June 30, 2015			**$ 206.24**

- The Agency maintains a bank account containing excess child support received for State wards that is more than the foster care maintenance amount. This bank account uses the State's FTIN but does not appear to have been established or approved by the State Treasurer, as of June 30, 2015, and was still not approved by the State Treasurer as of June 30, 2016.

Bank Name	Account Name or Owner	Account Number	Balance at 6/30/2015
West Gate Bank	DHHS – State Ward Child Support	XXX990	$ 1,359,665.61

- The Agency maintains eight bank accounts for the purposes of maintaining trust funds; neither the balances nor other information for these accounts were reported to the State Treasurer. These trust funds included bank accounts at the regional centers and the youth rehabilitation and treatment centers, as well as other State ward accounts. These bank accounts use the State's FTIN but do not appear to have been established or approved by the State Treasurer, as of June 30, 2015, and were still not approved by the State Treasurer as of June 30, 2016.

  Neb. Rev. Stat. § 43-907 (Reissue 2016) allows for these trust fund assets to be deposited into certain bank accounts for those children under the charge of the Agency. Neb. Rev. Stat. § 83-133 (Reissue 2014) allows for the investment of certain inmate trust funds related to those institutions under the control of the Agency. However, these funds remain subject to the State Treasurer's authority when it comes to establishing the banking relationships necessary for the creation of the depository accounts through which they must function and to ensure they are properly collateralized under the State's FTIN. The trust accounts are summarized below.

Bank Name	Account Name or Owner	Account Number	Balance at 6/30/2015	Account Location
Security First Bank	DHHS – Beatrice State Developmental Center	XXX240	$ 104,292.09	Beatrice State Development Center
U.S. Bank	State of Nebraska (DHHS)	XXX122	$ 65,826.47	Lincoln Regional Center
U.S. Bank	DHHS	XXX704	$ 60,784.76	Ward Trust Account
U.S. Bank	DHHS	XXX407	$ 45,317.26	Ward Trust Account
U.S. Bank	DHHS – Norfolk Regional Center	XXX586	$ 11,036.10	Norfolk Regional Center
Wells Fargo	DHHS – Youth Rehabilitation and Treatment Center	XXX033	$ 5,542.42	YRTC Kearney
Heartland Bank	DHHS – Youth Development Center Student	XXX041	$ 3,115.44	YRTC Geneva
Pinnacle Bank	DHHS – Hastings Regional Center – Patient Trust Fund	XXX363	$ 239.27	Hastings Regional Center
Total Balances at June 30, 2015			**$ 296,153.81**	

In addition to the duties of the State Treasurer under § 77-2301(1) and § 77-2309, as noted above, the Attorney General has stated in Op. Att'y Gen. No. 15-010 (Aug. 10, 2015), as mentioned already, "A state agency is not permitted to contract for its own banking relationship." This is because, that opinion declares, "The State Treasurer is charged with the duty of establishing the banking relationship for the State of Nebraska and its agencies."

Allowing bank accounts to be opened and operated under the State's FTIN without the authorization of the State Treasurer may result in loss or misuse of State funds or give rise to concerns regarding insufficient pledged collateral to secure the amount of public funds in excess of FDIC coverage.

> We recommend the Agency work with the State Treasurer to ensure all of its bank accounts are properly authorized. All bank accounts using the State's FTIN should be operated under the control or approval of the State Treasurer. The State Treasurer's approval should be documented and maintained on file.

Agency Response: Since the issuance of the prior audit early management letter, the Agency has been working closely with the State Treasurer's Office to review and authorize all accounts that will need to be retained for continued operations. The Agency has closed several of the accounts previously identified in the auditor's report. Updated signature cards have been obtained for all of the identified accounts in the prior audit. The Agency implemented new policies as well as an annual review process of external bank accounts. The Agency is currently working with the Treasurer on final authorization of the remaining accounts for which there has been a documented and Treasurer approved business need.

Simultaneously, the Agency is working with DAS to update accounting records for all petty cash funds with a business need. The Agency and DAS have worked to reconcile outdated EnterpriseOne accounting records to current information and are in the process of submitting finalized petty cash fund authorization forms.

The balance of the bank accounts noted in the audit report were not updated to reflect current balances. The excess child support account balances was reduced by moving funds into the state accounting system in coordination with the State Treasurer to ensure adequate collateralization of funds.

8. Account Balances Reported By the Agency

The APA requested all State agencies to report their financial accounts and respective bank account balances at June 30, 2015, as part of the audit work for the fiscal year 2015 CAFR and Statewide Single audits. As a result, the APA identified five Agency accounts for which the balances reported did not agree to the bank confirmation received. At the time of the 2015 CAFR audit work, the Agency Accounting Cost Manager was unsure why the balances did not match. Those variances had not been explained or resolved as of June 30, 2016:

Bank Name	Account Name or Owner	Account Number	Balance at 6/30/2015	DHHS Balance	Variance
Wells Fargo	DHHS – Youth Rehabilitation and Treatment Center	XXX033	$ 5,542.42	$ 3,878.40	$ 1,664.02
U.S. Bank	DHHS – Child Support Enforcement – Petty Cash	XXX313	$ 2,325.98	$ 1,977.00	$ 348.98
U.S. Bank	DHHS – Child Support Enforcement	XXX348	$ 2,038.68	$ 545.36	$ 1,493.32
Pinnacle Bank	DHHS	XXX038	$ 1,901.72	$ 1,551.95	$ 349.77
Pinnacle Bank	DHHS – Accounting Unit	XXX703	$ 1,283.20	$ 993.95	$ 289.25
Total Balances at June 30, 2015			**$ 13,092.00**	**$ 8,946.66**	**$ 4,145.34**

A good internal control plan and sound business practices require procedures to ensure accounting records agree to external documentation, such as bank statement balances.

When variances between bank account balances and accounting records are noted and not properly followed up on and corrected, there is an increased risk for loss or misuse of State funds.

> We recommend the Agency review and correct the specific bank accounts noted above. We also recommend the Agency implement procedures to ensure all bank account balances are reconciled to bank statements on a regular basis to ensure the accuracy of the reported balances. This reconciliation should identify variances the Agency can research and correct to ensure accounting records are accurate. The regular reconciliations should be documented and maintained on file.

Agency Response: The Agency will perform procedures to reconcile the identified accounts.

9. University of Nebraska Medical Center Medical Education Revolving Fund

In fiscal year 2015, the APA questioned disproportionate share hospital expenditures made from the University of Nebraska Medical Center Medical Education Revolving Fund (Fund). In establishing the Fund, Neb. Rev. Stat. § 85-134 (Reissue 2014) says, "The fund shall be used to fund medical education." During the year, the Agency expended a total of $15,846,757 from the Fund, including expenditures for disproportionate share hospital expenditures.

Neb. Rev. Stat. § 85-134 (Reissue 2014) provides the following, in relevant part:

> *The University of Nebraska Medical Center Medical Education Revolving Fund is hereby established to be administered by the Department of Health and Human Services. The fund shall be used to fund medical education.*

When the Agency processes expenditures from the fund other than those allowed by the unambiguous statutory language, it is not in compliance with State statute.

> We recommend the Agency comply with § 85-134 and if necessary, propose legislation that would allow disproportionate share hospital expenditures from the Fund.

Agency Response: The Agency will review the statute noted by the auditor and propose Legislative changes as appropriate.

10. Loss of Federal Funding

The Agency administers publically funded home and community based services and also operates several sites that provide services for individuals with developmental disabilities. The rates paid to the providers for these services are partially paid by Federal funds using the Federal Medical Assistance Percentage; the remaining expenses are paid with State funds. The Federal funds are provided by the Centers for Medicare and Medicaid Services (CMS). CMS must approve changes in program rates before expenses are reimbursed.

The Agency submitted expenditures for the State Ward Permanency Pilot Project but failed to modify its Medicaid waiver eligibility to include the project. As a result, $883,738 of expenditures submitted for reimbursement was ineligible for Federal reimbursement.

A similar finding was noted in the previous audit.

42 CFR § 441.304(d)(2) (October 1, 2015) provides the following, in relevant part:

> *A request for an amendment that involves a substantive change as determined by CMS, may only take effect on or after the date when the amendment is approved by CMS . . . .*

42 CFR § 441.304 (d)(1) states that substantive changes include changes in rate methodology.

Good internal controls and sound business practices require policies and procedures to ensure Federal waivers are submitted and approved timely prior to implementation of rates to ensure Federal expenditures are allowable.

When the Agency fails to comply with Federal requirements, and available Federal funding is lost, State general funds are required to cover these expenditures, resulting in an increased burden on Nebraska taxpayers.

> We recommend the Agency implement procedures to ensure compliance with all applicable Federal requirements to prevent the loss of funding.

Agency Response: The Division of Developmental Disabilities (DDD) self-identified this issue and worked to resolve this issue with our Federal Partner. DDD has created a Quality Assurance team that will be responsible for ensuring compliance with all State and Federal requirements. DDD has been working with the Centers for Medicare and Medicaid Services (CMS) over the last year to re-write the existing Home and Community Based Services (HCBS) Waivers for individuals with developmental disabilities. It is anticipated these new Waivers will take effect upon approval from CMS on March 1, 2017.

11. Timesheets

The Agency's overtime-exempt employees were not required to maintain documentation of actual time worked or certify that they worked at least 40 hours each week. Employees were required only to record leave used. As a result, there was nothing to support that staff rendered at least 40 hours of labor each week, as required by State statute, or that the hours worked by an employee were approved by his or her supervisor.

Neb. Rev. Stat. § 84-1001(1) (Reissue 2014) states the following, in relevant part:

> *All state officers and heads of departments and their deputies, assistants, and employees, except permanent part-time employees . . . 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.*

In addition, a good internal control plan requires that hours worked be adequately documented and approved, via timesheets or time logs, etc., and that such documentation be kept on file to provide evidence of compliance with § 84-1001(1).

Without adequate controls over payroll, there is an increased risk for payroll and leave balance errors, not to mention failure to comply with § 84-1001(1).

> We recommend the Agency implement procedures to document adequately employee hours worked or have the employee certify that the hours worked or leave used, or a combination thereof, totaled at least 40 hours each week. We also recommend implementing procedures to document supervisory approval of employee hours worked.

Agency Response: The Agency previously had implemented a system change within Kronos to ensure that all exempt employees certify that they worked at least 40 hours according to statutory requirements. This audit finding was limited to exempt employees at 24-hour facilities where the prior change did not take effect. That issue has been resolved and all exempt employees are now certifying time in accordance with State statute.

12. Business Continuity Planning

The Agency has established a Business Resumption Plan (BRP) but a completed Business Continuity Plan (BCP) or Continuity of Operations Plan (COOP) was not in place during the fiscal year ended June 30, 2016. Per discussion with Agency staff, the Agency has started the process of creating a COOP, but it is not complete.

The current BRP has not been adequately tested and does not include sufficient review of the Office of the Chief Information Officer (OCIO) COOP to ensure a comprehensive COOP is in place. Three of the key Agency computer systems reside on the OCIO mainframe: NFOCUS, which is used to automate benefit/service delivery and case management for over 30 Agency programs; CHARTS, which is used for Child Support Enforcement; and MMIS, which supports the operations of the Medicaid Program.

While NFOCUS, CHARTS, and MMIS reside on the OCIO's mainframe in a separate State building, the Agency has files and several software products that reside on Agency servers maintained at separate locations. These servers are included in the BRP.

A similar finding was noted during the previous audit.

COBIT 5, a business framework for the governance and management of enterprise information technology, lists the following management practices:

BAI10.01, "Establish and maintain a configuration model," states, in part, the following:

> *Establish and maintain a logical model of the services, assets and infrastructure and how to record configuration items (CIs) and the relationships amongst them. Include the CIs considered necessary to manage services effectively and to provide a single reliable description of the assets in a service.*

DSS04.03, "Develop and implement a business continuity response," states, in part, the following:

> *Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the enterprise to continue its critical activities . . . 4. Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity . . . .*

DSS04.04, "Exercise, test and review the BCP," provides the following:

> *Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.*

NITC Standards and Guidelines, Information Technology Disaster Recovery Plan Standard 8-201 (August 2006), Section 1, states: "The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency." This section notes, among others areas, that the plan must include an "[a]nnual plan review, revision, and approval process."

A good business continuity plan, which encompasses disaster recovery planning, includes making available reliable and useful information for decision making when faced with a disaster or other event causing or creating the potential for a loss of business continuity.

When a COOP plan is not complete and tested, there is an increased risk of extended downtime of vital State services.

> We recommend the Agency continue working to develop and implement a comprehensive business continuity plan.

Agency Response: The Agency has had a COOP plan developed for several years. The current COOP plan is undergoing updates to ensure alignment with the coordinated initiative to develop a state-wide COOP. We concur with recommendation of the need for updates and in cooperation with DAS, we have continued work on the Department/Division COOP plans including updates, testing, and training. Updated Division COOP plan drafts are due March 31, 2017. Anticipated completion of the Department and Division COOP plans is June 30, 2017. The Agency continues to coordinate the development of our COOP Plan in partnership with the DAS Continuity of Operations Administrator.

13. Med-IT User Access

The Agency uses the Med-IT application to support two Federally funded programs for the Office of Women's & Men's Health: Every Woman Matters Program and Nebraska Colon Cancer Program. Users are provided access to this application through 1 of 12 roles. Four of the 12 roles allow the user total access to the application, including the ability to make changes to roles, users, fees, program setup, and funding sources. For three of these four roles, users need this access to perform certain tasks in the system but do not need full access to the system. During testing, six employees were noted with access to these three roles, which allowed greater access than is commensurate with their job duties.

Additionally, one employee performs "Admin Reviews" of system access, which involve reviewing which parts of the Med-IT system users are using and if changes have been made by the user. However, there does not appear to be anyone reviewing that employee's access.

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

> *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 4.3.2.3, Separation of Duties, states the following:

> *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 and sound accounting practice include restricting access to information resources based upon job responsibilities to reduce the risk of unauthorized system access and to ensure access is commensurate with user job duties.

When users are granted inappropriate system access, significant information resources may be modified inappropriately, disclosed without authorization, and/or made unavailable when needed. 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 Federal funds being lost or sanctions imposed.

> We recommend the Agency continue to work towards developing a system with more defined permissions for the administrators and ensuring that users are provided with only the access needed to complete their job responsibilities. We recommend a formalized process be established for reviewing user access by someone who does not have access to the same functions.

Agency Response: The MED-IT system is not a software package customized only for the two identified programs, and as such any modifications could adversely impact other programs. Agency program staff have reviewed existing procedures and processes and feel that current checks and balances within the system are sufficient to prohibit unauthorized activity. Additionally, the Agency performs compensating controls in the form of administrative reviews as noted in the audit. The Agency has implemented an additional step to ensure the access of the administrative reviewer is adequately monitored.

14. CCF/MMF Tool User Access

The Agency uses the Change Control Facility/Migration Management Facility (CCF/MMF) tool for tracking changes made to the CHARTS, MMIS, and NFOCUS systems. The CCF/MMF tool is a mainframe application that maintains prior code versions in order to revert back to previous code. During a review of access to the CCF/MMF tool, eight users were identified who had access to check out code, develop a change, promote the change, and move the change into production.

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.9.11, Change Control Management, states the following:

> *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 & Guidelines, Information Security Policy 8-101, Section 4.3.2.3, Separation of Duties, states the following:

> *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 and sound accounting practice require application change approval to be completed by someone independent from the person who developed the change.

There is an increased risk that a change could be developed and moved into production by a single individual when adequate segregation of duties does not exist. There is also an increased risk of malicious coding being introduced into the production environment.

> We recommend the Agency implement procedures to ensure an adequate segregation of duties to prevent a user from developing a change and moving the change into production.

Agency Response: The Agency has reviewed the access for all eight users identified in the audit. Changes have been made to their CCF/MMF security to ensure adequate segregation of duties for all users. The Agency Application teams for CHARTS, NFOCUS, and MMIS have a formal change management process for making revisions to the applications. All program changes must be made in the development environment by a developer. A Configuration Management team member who has CCF/MMF promotion authority moves the code changes up the development chain. The changes go through system testing, client acceptance testing, and then when tested and approved it will be implemented into production by the Configuration Management team member. The Configuration Management members do not perform any type of changes to the program code. Quarterly reports are produced from the OCIO CCF Group on the list of approvers. This is reviewed quarterly by the Application Development Technical Supervisors.

15. NFOCUS User Access

The NFOCUS application is used to automate benefit/service delivery and case management for several Agency 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. In our review of employee access to NFOCUS, we noted the following:

- NFOCUS utilizes a Resource Access Control Facility (RACF), an IBM software product, which is a security system that provides access control and auditing functionality. There is a lack of segregation of duties in that a user with access to RACF profile DSSNFO07 can add an organization, create a service approval, create a service authorization, and enter the claim. Additionally, the profile DSSNFO07 has access to create a Master Case in NFOCUS.

    - In April 2016, the Agency implemented an exception report that notes a worker who created or modified an organization, created a service authorization, and created a service approval. The exception report does not note if a claim was entered by the same worker. The worker's supervisor is to review the actions taken by the worker noted on the exception report; however, this review was not documented.

- For 10 of 25 NFOCUS users tested, the level of user access was inappropriate for the user's job responsibilities, per the NFOCUS employee checklist or Agency support ticket.

- For 17 of 25 NFOCUS users tested, the NFOCUS Access Request Checklist or Agency support ticket was not properly completely or reviewed annually.

A similar finding was noted in the previous audit.

NITC Standards & 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."

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, provides the following, in relevant part:

> *A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts . . . . 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.*

The Supervisor Guide – Requesting NFOCUS access for user from the Security Administrator, states the following, in relevant part:

> *Instructions: Complete and sign the DHHS Internal Staff N-Focus Access Request Checklist and give to your local Security Administrator. Security Administrators are not permitted to complete the form for you and are instructed to return any incomplete or unassigned requests back to the requesting supervisor . . . .*
>
> *Once the checklist is signed and dated, the supervisor should make a copy to submit to the Security Administrator and retain the original for the employee's records.*
>
> *On an Annual basis the supervisors should review the employee's original request:*
>
> - *Is the current access still applicable?*
>
> - *If the access is still accurate, the supervisor should indicate the date review was completed on the original checklist.*
>
> - *If a change is needed, the supervisor should resubmit a new checklist with the accurate access needed.*

Without the proper completion of the NFOCUS Access Request Checklist, the Agency is unable to ensure that the user is assigned only to the access that is reasonable and necessary for the performance of the user's job duties. When users have access to applications that are unnecessary and unreasonable for the performance of their job duties, there is an increased risk for fraud and misuse of State funds. When one person has the ability to create an organization, create a service approval, create a service authorization, and then enter the claim, there is an increased risk for both unauthorized payments of claims and fraud.

We recommend the Agency establish procedures to ensure the NFOCUS Access Checklist is properly completed, maintained, and reviewed annually or when there is a change of assigned duties. For those who are granted access to NFOCUS without completing the NFOCUS Access Checklist, we recommend the Agency establish a formal policy and procedure to request, approve, and grant access to those employees and perform an annual review of user access. We recommend the Agency continue to establish procedures to have a documented review of users that may have created an organization, created a service approval, created a service authorization, and entered a claim in NFOCUS. We also recommend the Agency establish policies and procedures for verifying that previously requested access is no longer needed when such access does not appear on the most current checklist.

Agency Response: The Agency will implement a new annual control whereby Supervisors must attest that they have completed NFOCUS Access Request Checklists and annual appropriateness reviews of the Checklist for all direct reports that have NFOCUS access. The attestation mechanism would remind Supervisors of the need to retain a copy of the current NFOCUS Access Request Checklist and document the date of each annual checklist review with the employee's records. The Agency has implemented an Exception report that is ran weekly and identifies Users that have performed all three functions. The report is reviewed and the Users' Supervisor may be notified so they can verify whether the User's actions were appropriate or not. As most claims are paid monthly, if a claim is submitted it would be identified on this report before being paid.

16. External NFOCUS User Access

In our review of access to NFOCUS users, we noted that 9 of 51 external users tested at six external entities were no longer current and active employees of the external entity or no longer needed access to NFOCUS.

The APA requested contact information for 6 of 42 external entities for NFOCUS to determine if users were still active employees and needed access to perform their job duties. The entities selected and the results of this inquiry were as follows:

NFOCUS External Entities			
Entity	**Exceptions**	**Total Users**	**% Not Needing Access**
Midland Area Agency on Aging	3	19	15.8%
Douglas County Health Center	0	6	0.0%
Central Nebraska Child Advocacy Center	0	2	0.0%
League of Human Dignity, Inc.	4	13	30.8%
Food Bank of Lincoln	0	3	0.0%
Food Bank of the Heartland	2	8	25.0%
Total	**9**	**51**	**17.6%**

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, states the following, in relevant part:

> *A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (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.*

A good internal control plan requires terminated NFOCUS users' access to be removed timely.

The external entities did not communicate to the Agency when employees were terminated on a timely basis. The Agency performs a review of external users' access only once a year.

Failure to terminate user access to networks and applications timely creates the opportunity for unauthorized access to Federally protected State data.

> We recommend the Agency improve procedures by performing more routine reviews of external users' NFOCUS access in order to ensure unauthorized access is removed in a timely manner. We also recommend the Agency periodically inform external entities of the importance of notifying the Agency to remove employee access upon termination.

Agency Response: The Agency is implementing a new periodic report to identify external NFOCUS users that have not logged on to the system within the last 30 days. The new report will be used to request verification from the sponsoring Agency Program Division and the external entity that users on the report still require access to NFOCUS. In addition, the Agency will be enhancing the annual review of all NFOCUS external users to involve the program division sponsoring the external entity's NFOCUS access.

17. AB21 User Access

For two of eight user IDs selected for testing, the user's access to the Address Book 21 (AB21) role in EnterpriseOne was not reasonable and appropriate. Users with this role are authorized to maintain and update search types PH, XH, PM, XM, PW, XW (Public Assistance, Medicaid, Welfare) with Personal Data Security. This role also allows access to bank account information in these areas.

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, states the following, in relevant part:

> *A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (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.*

Failure to review or remove access to networks and applications when users no longer require such access creates the opportunity for unauthorized access and changes to data.

> We recommend the Agency establish procedures to review AB21 user access to determine if it is still reasonable and necessary for the employee's job duties.

Agency Response: The Agency will begin a standardized periodic review of all users with this EnterpriseOne access to ensure it is limited to users with a business need.

* * * * *

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 Agency 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 Agency.

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

Philip J. Olsen, CPA, CISA
Audit Manager