The University of Nebraska

Management Letter

For the Year Ended June 30, 2013

Issued on February 5, 2014

NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

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

December 13, 2013

The Board of Regents
University of Nebraska

We have audited the financial statements of the University of Nebraska (the University) (a component unit of the State of Nebraska) for the year ended June 30, 2013, and have issued our report thereon dated December 13, 2013.

Our audit procedures were designed primarily to enable us to form an opinion on the Basic Financial Statements. Our audit procedures were also designed to enable us to report on internal control over financial reporting and on compliance and other matters based on an audit of financial statements performed in accordance with government auditing standards and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the University's organization gained during our work, and we make the following comments and recommendations that we hope will be useful to you.

REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN AUDIT OF FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH *GOVERNMENT AUDITING STANDARDS*

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the financial statements of the business-type activities, and the discretely presented component unit of the University as of and for the year ended June 30, 2013, and the related notes to the financial statements, which collectively comprise the University's basic financial statements, and have issued our report thereon dated December 13, 2013. Our report includes a reference to other auditors who audited the financial statements of the University of Nebraska Foundation (Foundation), a discretely presented component unit of the University; the University of Nebraska Facilities Corporation, the UNMC Physicians, the University Technology Development Corporation, the University Dental Associates, and the Nebraska Utility Corporation, blended component units of the University (collectively identified as the Blended Component Units); and the activity relating to the Members of the Obligated Group Under the Master Trust Indenture, as described in our report on the University's financial statements. The financial statements of these entities were not audited in accordance with *Government Auditing Standards*.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

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. A *significant deficiency* is a deficiency, or a 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.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section 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. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified. We did identify a certain deficiency in internal control, described below, that we consider to be a significant deficiency: Comment Number 1 (SAP Transactions - Lack of Segregation of Duties).

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards.*

University's Response to Findings

The University's responses to our findings are described below. The University's responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

SCHEDULE OF FINDINGS AND RESPONSES

A. SIGNIFICANT DEFICIENCY

1. SAP Transactions - Lack of Segregation of Duties

A good internal control plan requires proper segregation of duties to ensure no one individual can process a transaction from beginning to end. A good internal control plan also requires a documented review of transactions before they are posted to the General Ledger (GL).

We noted a lack of segregation of duties in the processing of various types of transactions in SAP, which is the University of Nebraska's (University) accounting system. In addition, we also noted a lack of segregation of duties in the processing of various types of transactions in EnterpriseOne (E1), the State of Nebraska's (State) accounting system, which the University is required to use to process payroll and payments to vendors. Our audit noted the following:

Journal Entry (JE) Transactions in SAP

The workflow in the SAP system does not require separate preparers and posters of JE type transactions. As a result, certain individuals throughout the University had the capability of completing JE transactions from beginning to end without a documented secondary review and approval in SAP. The University did have a policy in place to review any JE transactions over $49,999, or $499 when involving Federal funds to address this inherent system weakness.

During our audit of the GL security roles in SAP for the fiscal year ended June 30, 2013, the Auditor of Public Accounts (APA) identified 561 users with the ability to prepare and post journal entries in SAP without a secondary review or approval. Additionally, one general ledger role allowed 73 users to prepare and post any transaction type in SAP without a secondary review or approval. (For further comment and recommendation on this area, see the Accounts Payable (A/P) Transactions section of this comment below).

The 73 users capable of preparing and posting JE transactions, as well as other transaction types, without a secondary review or approval are noted by location below:

Campus	# of Users
University of Nebraska at Kearney (UNK)	4
University of Nebraska-Lincoln (UNL)	28
University of Nebraska Medical Center (UNMC)	23
University of Nebraska at Omaha (UNO)	14
University of Nebraska Central Administration (UNCA)	4

When individuals are able to complete JE transactions (and other transaction types) without a documented secondary review and approval prior to posting the transaction to the GL, there is a greater risk of erroneous or inappropriate JE transactions (and other transaction types) occurring and going undetected. Additionally, in the absence of an adequate segregation of duties, there is an increased risk of loss, theft, or misuse of funds.

We recognize that the University has a policy to review higher risk journal entries to mitigate risks related to the SAP system not having an established workflow, which would automatically require a segregation of duties in the preparation and posting of journal entries (and other transaction types). Nevertheless, we continue to recommend the University implement a system-based SAP solution. Furthermore, we recommend that the University modify its role configuration for the 73 users identified, so that those users will not have the ability to post any transaction types in SAP without a secondary review and approval.

Management Response: The primary observation by the auditor wants an SAP-based solution to manage the role conflicts. The University has primarily relied on non-systems, materiality-based, manual processes, which the auditor acknowledges. Risk is further mitigated by the fact that most journal entries relate to cost distribution versus dealing with monetary assets. It should also be noted that the audit found no errors related to this observation. Management and those in governance are aware of this exposure and are willing to accept this low level of risk.

The auditor noted 73 users were assigned a general ledger security role granting broader transactional authorization. The audit comment indicates this security assignment authorizes the 73 users to enter any transaction. This, by itself, is not accurate as additional security roles are necessary to enter purchase orders, human resource appointments, and similar activities. The reference to 'any transaction' is misleading and should refer to 'any document type', which defines the type of general ledger entry being performed.

APA Response: The role security did not prevent a user from posting specific SAP transactions, therefore allowing an individual to complete transactions without a documented secondary review and approval prior to posting the transactions to the general ledger.

Accounts Payable (A/P) Transactions

A good internal control plan includes an adequate segregation of duties so no single individual has the ability to process an A/P transaction from beginning to end.

During our audit of the A/P security roles in SAP, we noted 42 users with the ability to prepare an invoice, post it in SAP, and approve and post it in E1. Additionally, 20 of those users had the ability to create a purchase order, prepare the invoice related to the purchase order, and post the transaction in both SAP and E1. Finally, we noted UNK staff posted parked documents without having the designed security role assigned to perform that function. As a result, we were unable to identify all users with the ability to post A/P documents in SAP.

The 42 users who could prepare invoices and post them in SAP and E1 are noted by location below:

Campus	# of Users
UNK	6
UNL	7
UNMC	13
UNO	10
UNCA	6

The 20 of the 42 users identified above who could also prepare a purchase order are noted by location below:

Campus	# of Users
UNK	3
UNL	0
UNMC	4
UNO	8
UNCA	5

The A/P roles in SAP did not restrict users from posting their own transactions. Those transactions were entered into E1 through an interface process. The users above had the ability to approve and post transactions that flowed through the interface process in E1.

Again, a lack of segregation of duties around the A/P process allows a single individual to purchase and pay vendors without a secondary review or approval. This risk allows for the possible theft and misuse of State funds.

> We recommend the University review the security design of the A/P roles in SAP and implement controls that require separate individuals to prepare and post A/P transaction types. We also recommend identifying how UNK was able to post parked documents without the assignment of the security role designed for that function.

Management Response: The University has strengthened controls in this area and will continue to do so. This is borne out by the fact that last year, it was observed that 69 persons could prepare and post payables entries. The number this year is 42. The existence of controls around overnight batching/matching of invoices, with matching done by an independent person reduces the chance of material errors. In addition, a batch integrity report was implemented by DAS in September 2013, further ensuring two or three users have reviewed vendor payments. It is our belief this internal control system also reduces the risk of fraudulent payments. These compensating controls are not acknowledged in the auditor's comments. We agree that this deserves continued efforts and will continue to seek solutions that will further diminish risk while being cost-effective.

Ability to Change Pay Rates

A good internal control plan includes an adequate segregation of duties, so no single individual has the ability to adjust his or her own pay rate. A good internal control plan also requires the

test environment of an application to mirror the production environment to ensure tests of the application functionality accurately predict the performance of the application in the production environment.

During a review of the human resources security roles in SAP, the APA identified 45 users with the ability to adjust their own pay rate in SAP. The HR role identified had a parameter set incorrectly, which allowed users to adjust their own pay. This issue was verified by the APA in the test environment; however, it could not be replicated in the production environment by the University staff. Therefore, the APA was unable to determine whether those users could actually adjust their pay rate in the production environment.

The 45 users with the ability to adjust their own pay rate in SAP are noted by location below:

Campus	# of Users
UNK	7
UNL	13
UNMC	10
UNO	11
UNCA	4

A lack of segregation of duties around the change of pay rates introduces the risk of possible theft and misuse of State funds. Moreover, when test environments do not function in the same manner as the production environment, there is an increased risk that tested controls and functionality will not work as designed.

> We recommend the University review the security design of SAP and implement controls that ensure an employee will not have the ability to change his or her own pay rate in SAP. We also recommend the University identify differences between the test and production environments.

Management Response: The auditor acknowledges University staff could not change their own pay rate in the SAP production system. This comment should be deleted as the production system does not permit a user to change their rate of pay.

APA Response: We acknowledge the University was unable to replicate the issue in the production environment. To our knowledge that testing was performed by the University for 2 of the 45 users noted who had "broad HR access." We believe a risk that someone could change their own pay rate still exists. More importantly, when test environments do not function in the same manner as the production environment, the effectiveness of SAP controls vetted through the testing process comes into question.

Management Response to Overall Comment: The University disagrees that this is a significant deficiency as the magnitude of a potential misstatement resulting from this comment is small and the reasonable possibility that controls will fail to prevent, detect, and correct a misstatement is low. The audit disclosed no misstatements of this nature.

APA Response: AICPA Auditing Standards, AU-C Section 265.07, defines significant deficiency as "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 in governance." We believe this finding merits attention by the Board of Regents and is appropriately identified as a significant deficiency in compliance with auditing standards.

Additionally AU-C Section 265.A5 states for when evaluating identified deficiencies in internal control, "Significant deficiencies and material weaknesses may exist even though the auditor has not identified misstatements during the audit."

B. BASIC FINANCIAL STATEMENTS MANAGEMENT LETTER COMMENTS

2. Expired Warrants

The University did not appear to have procedures in place to properly follow up on unclaimed (non-negotiated) warrants before expiration. The APA judgmentally selected five expired warrants over $5,000 for testing, and noted all five were not handled in compliance with Federal Regulations, Nebraska State Statutes, or Attorney General Opinions.

The following criteria apply to Federal, Trust, and Cash fund warrants, respectively:

- Per 34 CFR § 668.164(h)(2) (July 1, 2012), if a school attempts to disburse the credit balance due to a student for Federal financial assistance by check and the check is not cashed, the school must return the funds no later than 240 days after the date the school issued the check.

- Per Neb. Rev. Stat. § 69-1307 (Reissue 2009) and Op. Att'y Gen. No. 98043 (October 26, 1998), monies received by the State on behalf of another entity are to be treated as unclaimed property and are not payable to the General Fund upon expiration of the warrants.

- Neb. Rev. Stat. § 77-2205 (Reissue 2009) requires that the amount of a State warrant which remains un-cashed for more than one year after issuance shall be transferred to the State's General Fund unless "otherwise provided by law."

Of the five expired warrants we selected for testing, three were UNL Student Financial Aid Refund warrants, one was a UNK Student Financial Aid Refund warrant, and one was a UNO Trust Fund account warrant. With all five warrants selected for testing, the campuses did not follow up on the warrants before they expired.

> We recommend the University campuses implement procedures to follow up on outstanding warrants before they expire one year after issuance. Further, the campuses should comply with Federal and State regulations to remit the money to the proper agency before expiration.

Management Response: The University will continue to examine older state warrants for cancellation prior to the expiration date of one year after issuance. Outstanding warrants that are for student financial aid or another support entitlement will be returned to the appropriate source.

3. Outside Bank Account Activity

During fiscal year 2013, the balance in University outside bank accounts exceeded 2% of the balance in the University cash funds. In addition, we noted the activity in the accounts was excessive and indicative of depository accounts.

Neb. Rev. Stat. § 85-125 (Cum. Supp. 2012), § 85-192 (Cum. Supp. 2012), and § 85-1,123 (Cum. Supp. 2012) establish cash funds at UNL and UNMC, UNO, and UNK, respectively. These statutes all state the funds shall be in the custody of the State Treasurer, except that there may be retained by the Board of Regents, "a sum not to exceed two percent of the fund, which shall be available to make settlement and equitable adjustments to students entitled thereto, to carry on university activities contributing to the fund, and to provide for contingencies."

Neb. Rev. Stat. § 85-128 (Reissue 2008) states:

> *The State Treasurer shall be the custodian of all the funds of the university. Disbursements from the funds named in sections 85-124 to 85-127 shall be made in accordance with the provisions of law relating to the disbursement of university funds in the hands of the State Treasurer as provided by law.*

During fiscal year 2013, the APA noted the following activity in outside bank accounts at each of the University campuses:

	Credits	Debits
UNMC	$ 21,627,375	$ 21,700,432
UNO	$ 38,147,124	$ 38,426,881
UNL	$ 36,470,863	$ 36,743,532
UNK	$ 2,244,338	$ 2,229,741

The amount of outside bank account activity at each campus dropped from the prior fiscal year as the University began processing their credit cards through the State Treasurer. The transition of credit card processing began in May 2012 for UNMC, June 2012 for UNL, February 2013 for UNO, and March 2013 for UNK. However, the amount of activity in the outside bank accounts was still excessive and more indicative of a depository account rather than an account for the settlement of operating expenses.

Additionally, the APA noted that UNO exceeded two percent of the cash fund during these months in fiscal year 2013:

Month	2% of Cash Fund (at month end)	Balance in Outside Accounts	Amount Over 2% of Cash Fund
July 2012	$ 436,740	$ 451,933	$ 15,193
August 2012	179,248	598,982	419,734
September 2012	530,765	559,780	29,015
December 2012	371,696	509,216	137,520
January 2013	589,979	599,699	9,720

We noted a similar finding in our prior two audits.

We believe the University is not in compliance with State Statute in the way they utilize their outside bank accounts.

> We recommend that the University continue to work with the State Treasurer to determine the correct use of their outside bank accounts. We also recommend the University develop policies or procedures to ensure that the balances in the outside bank accounts are in compliance with State Statute.

Management Response: The University will continue to monitor the use of outside bank accounts and to use them only for the intended purpose of timely and equitable settlement with students, faculty, staff, vendors, and other external agencies. In doing so, the goal is to keep the balances in the accounts within the statutory 2% provision. The larger spike (balance) in the UNO account was a one-time phenomenon that occurred during the transition of certain activity to the State Treasurer depository account and was outside the normal course of business. We continue to make progress in this area as the activity in these accounts has decreased 40% over the past year.

4. Insufficient Pledged Collateral

Three campuses (UNO, UNL, and UNMC) did not acquire pledged collateral to cover their deposits when bank account balances exceeded the Federal Deposit Insurance Corporation (FDIC) coverage.

The FDIC's "Changes in FDIC Deposit Insurance Coverage" notes:

> *As scheduled, the unlimited insurance coverage for noninterest-bearing transaction accounts provided under the Dodd-Frank Wall Street Reform and Consumer Protection Act expired on December 31, 2012. Deposits held in noninterest-bearing transaction account are now aggregated with any interest-bearing deposits the owner may hold in the same ownership category, and the combined total insured up to at least $250,000.*

Neb. Rev. Stat. § 77-2395 (Reissue 2009) states:

> *1) If a bank, capital stock financial institution, or qualifying mutual financial institution designated as a depository furnishes securities pursuant to section 77-2389, the custodial official shall not have on deposit in such depository any public money or public funds in excess of the amount insured or guaranteed by the Federal Deposit Insurance Corporation, unless and until the depository has furnished to the custodial official securities, the market value of which are in an amount not less than one hundred two percent of the amount on deposit which is in excess of the amount so insured or guaranteed.*
>
> *(2) If a bank, capital stock financial institution, or qualifying mutual financial institution designated as a depository furnishes securities pursuant to subsection (1) of section 77-2398, the custodial official shall not have on deposit in such depository any public money or public funds in excess of the amount insured or guaranteed by the Federal Deposit Insurance Corporation, unless and until the depository has furnished to the custodial official securities, the market value of which are in an amount not less than one hundred five percent of the amount on deposit which is in excess of the amount so insured or guaranteed.*

(3) If a bank, capital stock financial institution, or qualifying mutual financial institution designated as a depository provides a deposit guaranty bond pursuant to the Public Funds Deposit Security Act, the custodial official shall not have on deposit in such depository any public money or public funds in excess of the amount insured or guaranteed by the Federal Deposit Insurance Corporation, unless and until the depository has provided to the custodial official a deposit guaranty bond in an amount not less than the amount on deposit which is in excess of the amount so insured or guaranteed.

A good internal control plan requires procedures to ensure all funds of the entity are fully covered through either FDIC coverage or pledged collateral, including obtaining confirmation from the third party banks holding the pledged securities.

We noted the following bank account activity in fiscal year 2013 for each campus:

Campus	Bank	# of Days over FDIC Coverage	$ Balance	Collateral Obtained	FDIC Coverage	Amount over FDIC Coverage & Pledged Collateral
UNO	First National	25	$320,289 - $1,578,187	$0	$250,000	$70,289 - $1,328,187
UNO	Wells Fargo	11	$251,711 - $364,835	$0	$250,000	$1,711 - $114,835
UNL	Pinnacle Bank	5	$779,952 - $1,554,964	$372,650	$250,000	$157,302 - $932,314
UNL	First National	4	$314,301	$0	$250,000	$64,301
UNL	Platte Valley Bank	12	$263,247 - $578,555	$0	$250,000	$13,247 - $328,555
UNL	Wells Fargo	2	$1,908,245 - $2,049,434	$1,641,641	$250,000	$16,604 - $157,793
UNMC	First National	6*	$262,728 -$786,726	$0	$250,000	$12,728 - $536,726

*UNMC bank statement format does not allow reader to easily determine specific days FDIC coverage was exceeded. We noted UNMC exceeded FDIC coverage on 6 of 24 bi-monthly statements.

> We recommend the University review bank account balances periodically to ensure pledged securities are maintained at all times to cover deposits, including obtaining confirmation from the third party banks holding the pledged securities.

Management Response: The University campuses will continue to seek collateral from their respective banks for balances exceeding the FDIC insurance limit. The collateral requirement will be discussed at least annually, or during periods of higher levels activity, with account representatives of banks entrusted with outside bank accounts.

5. Group Health Trust Fund and Payroll Vendor Payments

Many years ago, the University established a Group Health Trust Fund (Trust Fund) to provide for the investment and administration of contributions made pursuant to the University's Health Insurance Program (Program). The University's Trust authorizes BCBSNE and Caremark, the Program's third party administrators, to withdraw – with little, if any, oversight – funds directly from the Trust Fund for the payment of claims. In fact, under that broad grant of authority, those

third parties withdraw funds directly from the Trust Fund without either prior or subsequent University approval for each transaction.

On March 29, 2012, the APA issued an Attestation Report of the University of Nebraska Health Insurance Program. This finding was included in that report in significantly more detail than is included in this management letter. That report can be found on our website at:

http://www.auditors.nebraska.gov/APA_Reports/2012/SA51-03292012-July_1_2009_through_June_30_2010_Health_Insurance_Program_Attestation_Report.pdf.

Since 2003, the State has utilized E1 accounting software to record all of its official financial records in one centralized system. However, for more than a decade, the University has relied upon its own separate software, SAP, which is then interfaced with E1, for accounting purposes.

Payroll vendor payments are set up differently in SAP than in E1. Payments made to vendors through the State's payroll process are recorded as vendor payments in E1. However, instead of generating vendor payments through SAP or E1 during the payroll process, the University sends payroll payment instructions directly to the State's bank, authorizing the automatic deposit of payments to the vendors' banks. As a result, a vendor payment entry is not created in either accounting system; rather, only a journal entry is made to record such payments. Because the University's accounting system does not record vendor payments to health insurance vendors, such as BCBSNE, the total amounts paid to these vendors cannot be determined or identified by general users of the two systems.

The following amounts were contributed by the employees and the University through the University payroll process between July 1, 2012, and June 30, 2013:

Contributions	**University**
Health and Dental Insurance*	$ 117,879,349
TIAA/CREF (Retirement)	$ 71,400,882
All other contributions	$ 74,438,019
Total	**$ 263,718,250**

*The employee health insurance plan is self-insured. Currently the University's health insurance contributions go into a separate bank account.

Sound accounting procedures include complete and accurate reporting of all payments to vendors to allow users of E1 to review and report on all vendor payments. According to Neb. Rev. Stat. § 81-1110.01 (Reissue 2008), the purpose of the accounting division of the Department of Administrative Services is:

> *[T]o prescribe, coordinate, and administer a centralized, uniform state accounting and payroll system and personnel information system, to establish and enforce accounting policies and procedures for all state agencies, boards, and commissions, to monitor and enforce state expenditure limitations established by approved state appropriations and budget allotments, and to administer the federal Social Security Act for the state and the state's political subdivisions.*

When vendor payments do not originate from the State's accounting system, it is difficult for users of the system to ascertain the total amount paid to all vendors. This was noted as a finding

in the prior three fiscal years' audits. The University indicated they explored the possibility of interfacing the payments from SAP to E1; however, they concluded to continue with their current practice.

Based upon both the relevant State statutes and the Attorney General's opinions noted in the APA's Attestation Report referenced above, the APA still questions the authority, statutory or otherwise, of the University to establish the Trust Fund outside of the custody and control of the State Treasurer. As of June 30, 2013, the Trust Fund had a balance of $152,633,488.

> We recommend that the University consult with the State Treasurer to resolve this issue and join with the State Treasurer in seeking, if needed, a formal opinion from the Attorney General as to the legality of the Trust Fund's existence outside the custody and control of the State Treasurer. We also recommend the University work with the Department of Administrative Services to develop a process that allows vendor payments to be accurately recorded in the State's accounting system.

Management Response: The University is cognizant of an Attorney General's opinion that is dispositive on this issue: 1) the Group Health Trust funds are not monies of the State; 2) the establishment of the Trust is not contrary to laws designating the State Treasurer as custodian of University funds; and 3) the Trust falls under the Board's power to govern the University of Nebraska.

Accordingly, the recommendation should be removed from the letter.

APA Response: The Attorney General's opinion referenced by the University is Op. Att'y Gen. No. I-13015 (Dec. 20, 2013). Unfortunately, that opinion is merely an informal opinion and certainly far from conclusive; rather, it admits that "there is no clear answer" to the questions posed "absent some definitive case law from the Nebraska Supreme Court." Additionally, the University has always included the funds at issue on its own annual financial statements and reported them to the Department of Administrative Services – which is tantamount to acknowledging the public nature of that money. Until the Nebraska Supreme Court rules on this matter, the APA will continue to question the propriety of allowing the Trust Fund to impede the ability of the State Treasurer to exercise fully his statutory authority as the custodian of University funds.

6. Volleyball Camp Receipts Not Deposited Timely

During testing, we noted UNO did not timely deposit 23 checks received for volleyball camp registration.

Per Neb. Rev. Stat. § 84-710 (Reissue 2008):

> *It shall be unlawful for any executive department, state institution, board, or officer acting under or by virtue of any statute or authority of the state, including the State Racing Commission, to receive any fees, proceeds from the sale of any public property, or any money belonging to the state or due for any service rendered by virtue of state authority without paying the same into the state treasury within three business days of the receipt thereof when the aggregate amount is five hundred dollars or more and within seven days of the receipt thereof when the aggregate amount is less than five hundred dollars.*

A good internal control plan and sound business practices require that the University deposit receipts in a timely manner.

The Athletics Department hosted volleyball camps in July 2012 and received 23 checks totaling $7,690 from March 14, 2012 through July 9, 2012. However, it did not deposit the checks until July 18, 2012. See below for a summary of all checks received:

Check Date	Amount	Deposit Due	Deposit Made	Days Late
3/14/2012	$ 40	3/21/2012	7/18/2012	119 days
3/25/2012	40	4/1/2012	7/18/2012	108 days
3/25/2012	40	4/1/2012	7/18/2012	108 days
3/27/2012	40	4/3/2012	7/18/2012	106 days
4/12/2012	40	4/19/2012	7/18/2012	90 days
4/23/2012	40	4/30/2012	7/18/2012	79 days
4/23/2012	40	4/30/2012	7/18/2012	79 days
4/27/2012	40	5/4/2012	7/18/2012	75 days
4/29/2012	40	5/6/2012	7/18/2012	73 days
4/30/2012	40	5/7/2012	7/18/2012	72 days
5/3/2012	40	5/10/2012	7/18/2012	69 days
5/9/2012	40	5/16/2012	7/18/2012	63 days
5/21/2012	40	5/24/2012	7/18/2012	37 business days*
6/30/2012	140	7/4/2012	7/18/2012	10 business days
7/1/2012	140	7/4/2012	7/18/2012	10 business days
7/2/2012	165	7/5/2012	7/18/2012	9 business days
7/3/2012	5,705	7/6/2012	7/18/2012	8 business days
7/5/2012	165	7/10/2012	7/18/2012	6 business days
7/5/2012	320	7/10/2012	7/18/2012	6 business days
7/6/2012	40	7/11/2012	7/18/2012	5 business days
7/6/2012	140	7/11/2012	7/18/2012	5 business days
7/6/2012	140	7/11/2012	7/18/2012	5 business days
7/9/2012	215	7/12/2012	7/18/2012	4 business days

*Note that with the check dated 5/21/12, the cumulative amount of checks was $520, and thus the deposit on this date and all subsequent dates, by State Statute, were required to be made within *three business dates*. All checks prior to this date, by State Statute, were required to be made within *seven days*.

When receipts are not deposited in a timely manner, the University is not in compliance with State Statute, and there is increased risk of loss or misuse of funds.

> We recommend that the University implement procedures to ensure that deposits are made timely in compliance with § 84-710.

Management Response: The UNO campus agrees checks should be deposited timely when received at the counter or in the mail. The UNO Athletic Department is working with all the coaches involved to develop procedures to safe guard the custody of checks and improve timely deposits.

7. Student A/R and Alternative Loans Reconciliations

UNMC did not perform a reconciliation of alternative loans from Education Loan Management Resources (ELM) to SAP. Further, a reconciliation for student accounts receivable (A/R) in the Nebraska Student Information System (NeSIS) to SAP was performed but was inadequate.

A good internal control plan requires a reconciliation of amounts tracked by an outside system to the accounting system. A good internal control plan and sound business practices include procedures to ensure accounts receivable balances entered into SAP agree to the accounts receivable in NeSIS.

- Alternative Loans were processed by ELM and disbursed to UNMC. The funds are posted to SAP and to the student's account in NeSIS, which the University used to record, among other data, all tuition and fees charged to students. UNMC had not established a procedure to reconcile the amounts reported by ELM to the amounts recorded in SAP and NeSIS to ensure alternative loans were accurately reported in SAP.

- The process UNMC had in place to ensure student A/R balances in SAP agreed to student A/R balances in NeSIS was ineffective. UNMC was not able to provide adequate supporting documentation to show the student A/R balances for third party payments and outside scholarships recorded in SAP agreed to the corresponding balances recorded in NeSIS. Additionally, several of the reconciling items included on the reconciliations were supported only by an internal spreadsheet, not by reports directly from SAP or NeSIS.

Without an adequate reconciliation process in place, there is an increased risk for misuse of funds and inaccurate reporting.

> We recommend UNMC begin performing a reconciliation of ELM to SAP for alternative loans. Additionally, we recommend the campus improve procedures to ensure accounts receivable balances entered into SAP accurately reflect balances in NeSIS.

Management Response: The UNMC Student Services and General Accounting departments are collaborating to ensure balances between the general ledger and the Education Loan Management Resources System are reconciled and that reconciling items are cleared in succeeding accounting periods. The Student Services Department has changed the reconciling process of alternative loans. The reconciler will be a staff member who is not involved with the disbursement of alternative loans.

C. INFORMATION TECHNOLOGY (IT) MANAGEMENT LETTER COMMENTS

8. Password Parameters

Best business practices include establishing documented policies regarding minimum password standards to help adequately protect Information Technology (IT) resources. A good internal control plan includes system-enforced password parameters to ensure that users meet minimum password standards. A good internal control plan also includes a review of the changes made to the TrueYou Identity Manger, which is used by the University to enforce minimum password standards for SAP. The University campuses (except UNMC) also use TrueYou Identity Manager to enforce password standards for NeSIS. Changes to the TrueYou Identity Manager, especially large-scale changes, should be reviewed to ensure password levels are being assigned appropriately.

IT Governance Institute's Objectives for Information and Related Technology (COBIT 4.1), Process Control 5, *Policy, Plans and Procedures,* states:

> *Define and communicate how all policies, plans and procedures that drive an IT process are documented, reviewed, maintained, approved, stored, communicated and used for training. Assign responsibilities for each of these activities and, at appropriate times, review whether they are executed correctly. Ensure that the policies, plans and procedures are accessible, correct, understood, and up to date.*

There was no enterprise-wide password policy in place to require consistent password complexity settings among University campuses. Both SAP and NeSIS had password parameters and policies defined within various identity management systems; however, those parameters did not appear to be reasonable or consistent in comparison with other higher education and State government password policies currently in use.

UNMC utilized its own system to manage its password parameters for NeSIS; however, UNMC parameters were inconsistent with TrueYou Identity Manager settings and did not appear to be reasonable in comparison with other higher education and State government password policies currently in use. The password parameters at UNMC included password expiration set at 180 days, regardless of the level of access a user had.

We noted a similar finding in our prior audits. The APA was provided a draft copy of an enterprise-wide password policy for the University Computing Services Network with an initial draft date of January 13, 2013, and an intended effective date of July 31, 2013; however, this policy had not been approved or implemented.

When enterprise-wide policies are not established by management, there is an increased risk that password parameters set by various University IT staff will not be sufficiently strong and in line with management's intentions. Strong password parameters are essential to providing adequate security for information systems and protecting internal data. Weak password parameters increase the risk that unauthorized users may gain access to information systems and compromise the integrity and confidentiality of highly sensitive data.

> We continue to recommend the University develop, approve, and publish minimum enterprise-wide password standards. We recommend also that UNMC implement password settings that

require passwords to be changed every 30-90 days for all faculty and staff users who have access to sensitive or confidential data other than their own.

Management Response: It is the intent of the University to adopt a university-wide policy to establish password requirements and provide an overarching framework to establish minimum password requirements for the entire University. This password policy excludes the Affiliated Covered Entity Agreement between the University of Nebraska Medical Center and its healthcare partners as authorized per Executive Memorandum No. 27, which references its own password policy (Password Procedure Information Security Procedure). The password policy in place at UNMC complies with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, which establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."

All password construction requirements are to be defined in a manner that provides compliance with the applicable InCommon Level of Assurance (LOA): 1-Bronze or 2-Silver. The required LOA for a given system or user role will be determined by the information owner of that system, in cooperation with their entity Information Security Officer. The password construction requirements will include definition of required password length, complexity, duration, reusability, number of failed attempts allowed, and the lockout period after reaching that number of attempts. The desired combination of password construction factors must yield a level of entropy (complexity) sufficient to meet the minimum requirement for a given InCommon LOA, and be validated by InCommon endorsed tools for calculating password entropy. It is essential to understand that an acceptable entropy level may be achieved by various combinations of requirements (length, expiration, etc.) and that individual authentication systems may have differing password requirements while still meeting the required InCommon LOA.

While the current policies meet the foregoing best practices, work still continues to tighten controls around passwords. A draft of a new university-wide policy is in draft and under consideration. Once approved and finalized, the new password policy will be followed by all campuses for appropriate levels of authorization access to sensitive and confidential data.

9. NeSIS SACR Security Access

A good internal control plan includes processes, such as documented approval signatures, to ensure that only access required to perform job functions is granted to NeSIS users. Likewise, a periodic review of NeSIS user access should be performed to ensure that users are restricted to access required to perform their particular job functions.

During a review of individuals with access to modify Student Administration and Contributor Relations (SACR) security in NeSIS, it was noted that nine users (4 UNK and 5 UNMC) had access to modify security views. Such ability should be granted only to the UNCA NeSIS technical team.

Allowing security access to users who do not require such access as an essential part of their job duties increases the risk of unauthorized modifications to the system.

> We recommend the University remove campus user access to security views. We also recommend the University periodically review lists of users, especially those with privileged access to the system, to ensure their access is appropriate.

Management Response: A policy will be developed by the University Security Council for the appropriate data classification, access, and extraction that will be used by all campuses to protect sensitive and confidential data. This policy will ensure the privacy and protection of the data when it is extracted and downloaded by authorized users throughout the NeSIS community.

10. NeSIS Terminated User Access and SAP Terminations

The University of Nebraska Executive Memorandum No. 16, Section 5, states, in relevant part:

> *Unauthorized access to information systems is prohibited…When any user terminates his or her relation with the University of Nebraska, his or her ID and password shall be denied further access to University computing resources.*

A good internal control plan requires that terminated NeSIS user access be removed timely. Additionally, documentation – whether by system audit records, access removal forms, or both – should be available to indicate that such access was properly removed.

NeSIS Terminated User Access

For 16 of 21 University terminations tested, NeSIS access was not removed within three business days following termination. One additional terminated employee noted in the prior audit still had NeSIS access. In addition, UNL's process for removing access was not sufficient to ensure timely removal of access for terminated users. UNL staff were notified of terminations on a monthly basis through an SAP terminations report. As a result a UNL employee terminating at the beginning of a month retained access until the beginning of the following month. See table below:

Number of Terminated Employees	Campus	Access Removed Calendar Days After Termination
1	UNCA	7
1	UNK	Over 120
7	UNL	12 to 315
1	IANR	9
1	UNMC	Over 357
6	UNO	24 to 448

SAP Terminations

For 3 of 25 terminations tested, SAP access was not removed within three business days after termination. See table below:

Number of Terminated Employees	Campus	Access Removed Calendar Days After Termination
1	UNL	15
2	UNMC	17 and 164

Based on our understanding of the SAP access removal process for terminated employees, the lack of timely removal of access was due to the separation dates not being entered into SAP in a timely manner. Additionally, 'non-payroll relevant' users were not included in batch runs used to remove user access. We noted a similar finding in our prior audits.

When terminated user access to networks and applications is not removed in a timely manner, it creates the opportunity for unauthorized processing of transactions.

> We recommend the University implement a formal procedure to ensure appropriate staff are notified of all terminations in order to remove terminated user access to NeSIS within three business days and that this procedure be documented. We also recommend the University enter separation dates into SAP immediately in order to ensure the timely removal of access to networks and applications for terminated users. Finally, we recommend developing procedures to ensure "non-payroll relevant" users access is removed in a timely manner.

Management Response:
NeSIS Terminations: The campuses and the NeSIS staff have removed the access of the users identified who should not have access to NeSIS and continue to work on improved procedures for the removal of terminated users. These procedures will include documentation and a time stamped log of terminated staff prepared on a timely basis from the NeSIS system. Additionally, the University is working on an enhanced Terminated User Report to be used by the NeSIS security coordinators. Once completed, this report will provide the NeSIS security coordinators information of HR actions pertaining to NeSIS business end-users, thus allowing improved, timelier information to determine when to remove access.

SAP Terminations: The SAP administrative systems group will follow up with the campus Human Resource offices to emphasize the importance of entering separations in a timely manner. The observation that non-payroll relevant users are not included in the automated separation process is incorrect; the programs make no distinction based upon payroll status.

APA Response: During our testing, the cause of the two terminated UNMC users whose access was not removed in a timely manner was identified by University staff as an issue

with the batch process used to remove user access. Specifically, University staff noted that those users were payroll area 99, (non-payroll relevant), and that those users were not included in the batch process. If the University has now determined otherwise, the fact that the users' access was not removed in a timely manner remains unchanged.

11. Financial Aid Segregation of Duties

A good internal control plan requires an adequate segregation of duties, so no single individual has the ability to create a scholarship, configure scholarship parameters, and award the scholarship to a student.

There were 13 University users (4 UNMC and 9 UNCA) with the ability to set up a specific student, create a scholarship, configure the scholarship parameters, and then award that scholarship to the student in NeSIS.

A lack of segregation of duties around the creation and application of scholarship awards increases the risk of a single individual setting up and applying awards to students without a secondary review or approval.

> We recommend the University implement an adequate segregation of duties around the scholarship award process, so a single individual is not able to create a scholarship, configure the scholarship parameters, and then award the scholarship to a student, particularly if those users can also create a student in NeSIS.

Management Response: The campuses and the NeSIS administrative group have initiated a security re-design task to address the segregation of duties requirements for scholarship award processing. Once completed, the new security policy for processing scholarships will be implemented for all University campuses.

12. NeSIS Data Extraction

A good internal control plan includes adequate policies and procedures to ensure student information is safeguarded against security risks associated with storing extracted data from NeSIS. Safeguards include an inventory of data locations, an inventory of data stored by departments, preventing student information databases from residing on mobile computing devices (including laptops, tables, phones, and flash drives), and adequate logical and physical controls.

The University allowed department level staff to extract student information from NeSIS (via WebFOCUS) for use in their own databases. This data was used for analysis, reporting, statistics, etc. and may have been combined with data from other department sources. There was no policy or process in place to document who extracted data, what was extracted, where the data was stored, or how the student data was protected from security threats.

A lack of policies and procedures around safeguarding student information introduces an increased risk for lost, stolen, and hacked data.

> We recommend the University create policies and procedures to ensure student information extracted to department level databases is adequately safeguarded.

Management Response: A policy will be developed by the University Security Council for the appropriate data classification, access, and extraction that will be used by all campuses to protect sensitive and confidential data. This policy will ensure the privacy and protection of the data when it is extracted and downloaded by authorized users throughout the NeSIS community.

* * * * *

It should be noted that this letter is critical in nature, as it contains only our comments and recommendations and does not include our observations on any strengths of the University.

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

This letter is intended solely for the information and use of management, the Board of Regents of the University of Nebraska, others within the University, and the appropriate Federal and regulatory awarding agencies and pass-through entities, and it is not intended to be, and should not be, used by anyone other than these specified parties.

Sincerely,

SIGNED ORIGINAL ON FILE

Mark Avery, CPA
Audit Manager