The University of Nebraska

Management Letter

For the Year Ended June 30, 2015

This document is an official public record of the State of Nebraska, issued by the Auditor of Public Accounts.

Modification of this document may change the accuracy of the original document and may be prohibited by law.

Issued on February 9, 2016

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

December 8, 2015

The Board of Regents
University of Nebraska

We have audited the financial statements of the University of Nebraska (University), a component unit of the State of Nebraska, for the year ended June 30, 2015, and have issued our report thereon dated December 8, 2015.

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, 2015, 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 8, 2015. 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, the UNeHealth, 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 the Foundation, the University of Nebraska Facilities Corporation, the UNMC Physicians, the University Dental Associates, the UNeHealth, and the

Nebraska Utility Corporation were not audited in accordance with *Government Auditing Standards* and accordingly, this report does not include reporting on internal control over financial reporting or instances of reportable noncompliance associated with these entities.

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. 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.

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

1. Revenue Reconciliations & Collection Procedures

The University did not perform adequate reconciliations of the accounting system (SAP) to outside systems at two campuses.

- UNMC performed a reconciliation of alternative loans from Education Loan Management Resources (ELM) to the Nebraska Student Information System (NeSIS), but the reconciliation was inadequate. It was noted that the reconciliation did not include an adequate review of the SAP balance. Alternative loans are processed by ELM and disbursed to UNMC, and the funds are posted to SAP and to the student's account in the NeSIS, which the University uses to record, among other data, all tuition and fees charged to students.

- UNL and UNMC performed a reconciliation of accounts receivable (A/R) in NeSIS to SAP, but the reconciliation was inadequate. UNMC's reconciliation process was ineffective, as it was unable to provide adequate supporting documentation to show that A/R balances for third-party payments and outside scholarships recorded in SAP agreed to the corresponding balances recorded in NeSIS. UNL's reconciliation process was also ineffective, as it was unable to reconcile the amount in SAP to the amount in NeSIS and, therefore, recorded an unsupported reconciling item of $287,943 in SAP for the variance between SAP and NeSIS.

In addition, adequate collection procedures for student receivables were not followed at UNK, UNL, and UNO. Ten student accounts receivables were tested at each of those campuses.

- At UNK, one student had an uncollected balance of $3,049 for Fall 2014. The student was not identified on the UNK past due service indicator report which resulted in UNK not following the appropriate procedures for overdue accounts.

- For one student at UNL, the receivable balance of $4,562 from Fall 2014 had not been sent to collections, as it was overlooked due to human error.

- At UNO, one student had an outstanding balance from Summer 2014 and Fall 2014 of $2,839; however, after completing a one-time payment agreement, the student was allowed to enroll in classes for Spring 2015. The student's balance remained unpaid after the Spring 2015 semester and a subsequent balance of $1,528 was added for the Spring 2015 semester. The collections process did not begin in a timely manner.

A good internal control plan and sound business practices require procedures to ensure performance of a timely reconciliation of amounts tracked by an outside system to the accounting system. Sound business practices and a good internal control plan also require procedures to ensure adequate collection activities occur for individuals with delinquent balances.

Without an adequate reconciliation process in place, there is an increased risk for misuse of funds or inaccurate reporting. When collection procedures are not in place and followed, there is an increased risk of student account balances remaining uncollectible.

A similar finding was noted in our prior audits.

> We recommend UNMC continue performing the alternative loans reconciliation and improve its current procedures to include a review of the SAP balance. We also recommend UNL and UNMC improve procedures to ensure accounts receivable balances entered in SAP accurately reflect balances in NeSIS. Finally, we recommend the University review accounts with outstanding balances to ensure the procedures are followed for balances remaining uncollectible.

Management Response: *UNMC completed the reconciliation procedures on June 30, 2015. A collaborative project is underway including Student Accounts and the Controller's Office to strengthen third party receivable processing and accounting reconciliation by June 30, 2016.*

UNL has undertaken an initiative to clearly support reconciling items between the SAP general ledger and NeSIS.

2. Audit Differences

A good internal control plan and sound accounting practices require financial information to be complete and accurate. This includes procedures to ensure the financial statements are correct, and adjustments are made to rectify all known significant ($1,000,000 or more) misstatements.

During our audit of the financial statements, we noted several errors that resulted in significant misstatements. We proposed the University adjust its statements to correct all of these errors; however, the University made only some of the proposed corrections.

The following are significant misstatements the University corrected:

- A UNMC accounts payable entry to accrue retainage on a construction project was over-accrued by $8,164,821.

- A UNMC subsequent construction disbursement selected for testing, totaling $9,187,388, should have been accrued as an account payable but was not.

- UNMC did not consistently blend other current accounts receivable of UNMC Physicians (UNMC-P), a blended component unit of UNMC, into its consolidated financial statements. It reflected UNMC-P's $4,192,195 fiscal year 2014 other current accounts receivable as Other Assets but classified UNMC-P's $4,031,856 fiscal year 2015 other current accounts receivable as Accounts Receivable.

- UNL did not properly record the accounts receivable and deferred inflows of resources associated with its Follett bookstore service concession arrangement. The campus should have recognized a total of $4,471,846 in Accounts Receivable and $4,471,846 in Deferred Inflows of Resources in fiscal year 2015 in connection with this agreement. However, it incorrectly used the fiscal year 2014 amount from a supporting worksheet, $5,962,462, for both of these line items. Thus, both of these line items were overstated by $1,490,616.

The following are significant misstatements the University did not correct:

- UNO recorded a capital grants and gifts receivable for the arena project in fiscal year 2013. Therefore, when the revenue was actually received in fiscal year 2014, it should have been recorded to Capital Grants & Gifts but was recorded to Other Transfers. As a result, the fiscal year 2014 Capital Grants & Gifts revenue was understated by $1,088,403, and Other Transfers was overstated by $1,088,403.

- UNMC recorded an accounts receivable and an unearned revenue in fiscal year 2014 for Fall 2014 tuition and fees, but they were not due until after the 2014 fiscal year end. This resulted in both Accounts Receivable and Unearned Revenue being overstated by $3,472,517 for fiscal year 2014.

- Following financial statement preparation, UNMC recorded any paper adjustments in SAP. While booking the adjusting journal entry to move fiscal year 2014 revenue from Federal Grants & Contracts to Unearned Revenue, UNMC made the entry to State and Local Grants & Contracts rather than to Federal Grants & Contracts. This entry did not affect the fiscal year 2014 financial statements. However, during fiscal year 2015, the entry automatically reversed and resulted in State and Local Grants & Contracts being overstated by $2,216,489 and Federal Grants & Contracts being understated by $2,216,489.

- The balance of the University of Nebraska's reimbursement account of employee deductions was not recorded on its financial statements. Therefore, Cash and Accounts Payable were understated by $1,687,582 for fiscal year 2014 and by $1,039,909 for fiscal year 2015.

- UNK restated its fiscal year 2014 Statement of Revenue, Expenses, and Changes in Net Position (SRECNP), but this restatement was not reflected in the consolidated University-wide SRECNP. UNK reclassified $1,794,130 in fiscal year 2014 revenue from Sales & Services of Auxiliary Operations to Tuition & Fees revenue. It also reclassified $1,108,586 in fiscal year revenue from Sales & Services of Educational Activities to Tuition & Fees revenue. However, the restatements were not reflected on the fiscal year 2014 University-wide SRECNP.

- UNMC restated its fiscal year 2014 SRECNP, but this restatement was not reflected in the consolidated University-wide SRECNP. UNMC reclassified $1,405,639 in fiscal year 2014 revenue from Private Grants & Contracts – Restricted to Investment Income. However, the restatement was not reflected on the fiscal year 2014 University-wide SRECNP.

- UNL double recorded revenue for alternative student loans. Revenue was recorded to multiple revenue line items when students signed up for classes and an Accounts Receivable was subsequently recorded. When the money from the third-party loans was received, it was also recorded as revenue to Private Grants & Contracts instead of as a reduction in Accounts Receivable. The University then made an entry to reduce Accounts Receivable; however, instead of removing the second revenue, they recorded an expense. Therefore, the total amount of revenue overstated in the financial statements due to improper accounting was $7,935,492, and expenses were also overstated by this same amount.

A similar finding was noted in our prior audit.

Without strong internal control procedures and accounting practices to ensure financial information is complete, accurate, and in accordance with accounting standards, there is a greater risk material misstatements may occur and remain undetected. Although significant, these uncorrected errors did not result in a modification of our opinion on the financial statements.

> We recommend the University implement procedures to ensure financial information is complete, accurate, and in accordance with accounting standards. We further recommend the University make financial statement adjustments for all known significant misstatements.

Management Response: *It should be noted that the misstatements listed by the auditor have zero impact on net position or net assets. In our terminology, we call the items listed "reclassifications" as they move balances from one line item to another or in the case of two entries, gross up the statement of financial position to reflect accounts held on behalf of employees. We will re-examine the close process to determine how to better capture reclasses made at the campus level in creating the combined statements.*

APA Response: The evaluation of the fair presentation of the financial statements is based on not only the Net Position line item, but also on the fair presentation of all financial statement items presented.

Generally Accepted Auditing Standard AU-C 450.04 discusses evaluating misstatements identified and defines misstatements as a difference between: the amount, classification, presentation, or disclosure of a reported financial statement item and that which is required for the item to be presented fairly in accordance with the applicable financial reporting framework.

3. Outside Bank Account Activity

During fiscal year 2015, the activity in University outside bank accounts was excessive and indicative of depository accounts.

Neb. Rev. Stat. § 85-125 (Reissue 2014) and § 85-192 (Reissue 2014) establish cash funds at UNL and UNMC, and UNO, respectively. Both of these statutes require the funds to be in the custody of the State Treasurer, except that the Board of Regents may retain "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 2014) states the following:

> *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 2015, the APA noted the following activity in outside bank accounts at each of the University campuses:

	Credits	Debits
UNMC	$ 15,094,455	$ 15,024,084
UNO	$ 5,874,622	$ 5,937,382
UNL	$ 29,304,149	$ 29,896,202

The amount of outside bank account activity dropped from the prior fiscal year at all three campuses. 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.

A similar finding was noted in our prior audits.

> We recommend the University continue to work with the State Treasurer to determine the correct use of its outside bank accounts.

Management Response: *The University will continue to monitor and evaluate its outside bank accounts in accordance with state statutes which allows accounts and funds "to make settlement and equitable adjustments to students entitled thereto, to carry on university activities contributing to the fund, and to provide for contingencies".*

4. University of Nebraska at Omaha (UNO) Dome Revenues

UNO lacked adequate internal controls over the billing and collecting of revenues generated from the UNO Dome. In addition, two UNO Dome revenue entries selected for testing lacked adequate supporting documentation and contained errors.

Good internal control requires a plan of organization, procedures, and records designed to safeguard assets and provide reliable financial records. A system of internal control should include a proper segregation of duties, so no one individual is capable of handling all phases of a transaction from beginning to end.

We noted the following internal control issues over the UNO Dome revenues:

- There is a lack of segregation of duties over the UNO Dome billing process. The Business Manager of Campus Recreation Facilities is responsible for most of the financial activities of the UNO Dome, including creating the invoices, receiving the payments, and maintaining the spreadsheet that tracks the payments.

- UNO's policy is to charge organizations only for the days they use the Dome, not the days they reserve the Dome. The Facility Reports document whether organizations used the UNO Dome on the days they reserved it. The Facility Reports were not provided to the Business Manager, the preparer of the invoices, and were not used in the preparation of the invoices.

- The Facility Reports also did not consistently document whether the Dome was used by the organizations. The Facility Reports for January through April 2015 were reviewed and it was noted that 17 reservations, totaling 33.50 hours, were not documented as to whether or not the organization used the Dome.

- The current fee sheet, which has been in use for the past two years, was not reviewed or approved by the Director of Campus Recreation until September 22, 2015.

- There was no documented legal review of the contract template.

The UNO Dome revenue entries selected for testing, comprised of five invoices, lacked adequate supporting documentation and contained errors.

- Three invoices had contract rates that did not agree to the fee sheet, and there was no documentation for the difference.

- One invoice charged one hour for Dome use when the Facility Report documented that the organization did not use the Dome on that day, which resulted in the organization being overcharged $170.00.

- Two invoices had six hours total ($1,020) that did not have documentation on the Facility Reports as to whether or not the organization used the Dome on those days.

A similar finding was noted in our prior audit.

> We recommend the University review the procedures for the UNO Dome and implement strong internal controls over the billing and collecting of revenues. We also recommend the fee sheet and any updates thereto be reviewed and approved. We further recommend the legal department review the current contract template used by the UNO Dome. Finally, we recommend the Facility Reports consistently document the Dome usage by organizations.

Management Response: *Dome revenues are very insignificant to the University's financial position. However, the University will improve the adherence to procedures for the Dome invoicing, approval of rates, documentation, and contract management as well as ensure proper internal controls at HPER.*

5. Group Health Trust Fund

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).

On March 29, 2012, the APA issued an Attestation Report of the University of Nebraska Health Insurance Program. That prior 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

The APA continues to question the underlying authority, statutory or otherwise, of the University to establish the Trust Fund outside of the custody and control of the State Treasurer. This skepticism is based upon both the relevant statutes and the Attorney General's opinions noted in the above-mentioned Attestation Report of the University of Nebraska Health Insurance Program, which the APA issued in 2012.

In the previous two years, the University made reference to an informal Attorney General's opinion regarding the Trust Fund, Op. Att'y Gen. No. I-13015 (Dec. 20, 2013). We note, however, that this is merely an informal opinion and certainly far from conclusive; rather, it admits "there is no clear answer" to the questions posed "absent some definitive case law from the Nebraska Supreme Court."

Additionally, the University has always (and continues to) include the funds at issue on its own annual financial statements, reporting them as an Unrestricted Net Position, as well as reporting them to the Department of Administrative Services, which is tantamount to acknowledging the public nature of that money. Until the State Treasurer grants approval or 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.

As of June 30, 2015, the Trust Fund had a balance of $145,139,979.

> We recommend the University consult with the State Treasurer – and, if necessary, seek jointly a formal opinion from the Attorney General – to resolve the ongoing issue regarding the legality of the Trust Fund's existence outside the custody and control of the State Treasurer.

Management Response: *As stated in prior responses, the University considers the health trust fund ownership question closed. On December 20, 2013, the Nebraska Attorney General Office issued opinion No. I-13015 which provided 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 power of the Board of Regents to govern the University of Nebraska.*

APA Response: As noted in previous APA comments addressing this issue, the informal Attorney General's opinion referenced by the University is, per its own admission, far from conclusive. Moreover, the State Treasurer has recently reiterated his concurrence with the APA's long-standing analysis, agreeing that the University's maintenance of the health trust fund violates both State law and his own constitutional authority. Therefore, the University's insistence that the matter is "closed" appears premature.

6. Contracts not on the State Contracts Database

Neb. Rev. Stat. § 84-602.02(3)(a) (Reissue 2014) states the following:

> *Beginning July 1, 2014, the web site described in this section shall include a link to the web site of the Department of Administrative Services. The department's web site shall contain: (i) A data base that includes a copy of each active contract that is a basis for an expenditure of state funds, including any*

> *amendment to such contract and any document incorporated by reference in such contract. For purposes of this subdivision, amendment means an agreement to modify a contract which has been reduced to writing and signed by each party to the contract, an agreement to extend the duration of a contract, or an agreement to renew a contract. The data base shall be accessible by the public and searchable by vendor, by agency, board, commission, or department, and by dollar amount. All agencies, boards, commissions, and departments of the state shall provide to the Department of Administrative Services, in electronic form, copies of such contracts for inclusion in the data base beginning with contracts that are active on and after January 1, 2014 . . . .*

We tested 19 expenditures governed by contracts and noted 7 of the contracts were not included on the State Contract Database, as required by State statute. Three of five of those contracts were at UNL; one was at UNCA; 1 of 2 was at UNK; 1 of 4 was at UNMC; and 1 of 7 was at UNO.

> We recommend the University include all of its contracts on the State Contracts Database in a timely manner to stay compliant with State statute.

Management Response: *The University will strive to continue filing contracts in the State Contracts Database on a timely basis.*

7. General Ledger Transactions in SAP

A good internal control plan requires a proper segregation of duties to ensure no one individual can process a transaction from beginning to end. A good internal control plan also includes adequate security controls, through the design, creation, approval, and assignment of user roles, to prevent users from performing functions that do not allow for a proper segregation of duties.

The workflow in the SAP system does not require separate preparers and posters of General Ledger (GL) type transactions, primarily journal entries that do not result in vendor payments. As a result, certain individuals throughout the University had the capability of completing GL 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 journal entries (JE), payroll journal entries (PJ), NIS (refers to E1) journal entries (ND), University-only journal entries (UU), and non-Federal ACH receipt (CN) transactions over $49,999, or $499 when involving Federal funds, to address this inherent system weakness.

A similar finding was noted in our prior audits.

During our audit of the GL security roles in SAP, we identified 579 users with the ability to prepare and post GL entries in SAP without a system required secondary review or approval. The 579 users capable of preparing and posting GL transactions without a secondary review or approval are noted by location below, along with the GL document types they could prepare and post:

Campus	# of Users
UNK	4
UNL	311
UNMC	190
UNO	61
UNCA	13

(Document Types: JE, IB-Internal Charges Batch, IC-Internal Charges Online, and PJ)

A secondary role allowed 75 of those users to prepare and post additional GL document types. The 75 users capable of preparing and posting additional GL document types without a system required secondary review or approval are noted by location below, along with the GL document types they could prepare and post:

Campus	# of Users
UNK	4
UNL	29
UNMC	22
UNO	15
UNCA	5

(Document Types: CN, ND, UU, UA-Accrual Journal Entry, and TN-Interstate Billing Transaction)

When individuals are able to complete GL transactions without a system required secondary review and approval prior to posting the transaction to the GL, there is a greater risk for error and inappropriate GL transactions to occur and remain 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 general ledger transactions 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 general ledger entries. Nevertheless, we continue to recommend that the University modify its role configuration for the 579 users identified, so that those users will not have the ability to post any GL transaction types in SAP without a system required secondary review and approval.

Management Response: *We believe a secondary approval of journal entries contributes minimally to controlling material financial risk and disagree with this recommendation. We believe the following University administrative practices mitigate the financial risks associated with journal entries. First, certain journal entry transaction codes are reviewed if the entry is posted to Federal funds and the dollar amount exceeds $500 and reviews all other entries if the dollar amount exceeds $50,000. Second, departments verify posted charges, including journal* *entries, reducing the risk of inappropriate entries. Third, grants officers review charges when preparing Federal grant expenses reports. Finally, risk is further mitigated by the fact that journal entries primarily relate to cost distribution rather than adjusting the values of monetary assets. It should also be noted the audit once again found no errors related to this comment.*

8. <u>NeSIS Financial Aid Segregation of Duties</u>

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, especially when that individual can also set up a new student.

Eight users at UNCA, one user at UNMC, and one consultant had 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. The UNCA users were IT staff with a high level of access. In addition, seven users (four at UNMC and three at UNL) had the ability to create a scholarship, configure the scholarship parameters, and then award that scholarship to a student in NeSIS. Two additional users (one at UNO and one at UNMC) had access to create a scholarship, award a scholarship, and set up a student.

A similar finding was noted in our prior audits.

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 in 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 the user can also create a student in NeSIS.

Management Response: *The University planned for an additional NeSIS technical resource and a person was hired in December 2015. This individual will work with the campus security coordinators and business communities to design and build these new security roles that will be offered and implemented to all other campuses. The usage and assignment of these new segregated roles will be made by each campus Financial Aid Director and their respective NeSIS campus security coordinators.*

9. <u>NeSIS Improper Access</u>

A good internal control plan includes a periodic review of users' access to ensure that users are restricted only to access that is required as part of their job function.

The University of Nebraska Executive Memorandum No.16 (Section 5) states, "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."

InCommon Identity Assurance Profiles: Bronze & Silver (February 11, 2013), Section 4.2.4.2, states, "The IdPO shall revoke Credentials within 72 hours after being notified that a Credential is no longer valid or is compromised." Human resources staff is involved in notifying the Identity Provider Operator (IdPO) of terminations and should work to achieve access removal within a 72-hour period.

A good internal control plan also requires terminated user access be removed timely and documented, whether by system audit records or access removal forms, or both, be available to indicate that access was properly removed.

During a review of NeSIS roles that provide significant system access, a student records role was identified that had access to modify enrollment data across all campuses without being tracked or logged. This role was initially intended to be utilized on a temporary basis, as needed; however, most of the 10 University users with this role had it for nearly three years (6 UNO, 2 UNK, 1 UNL, and 1 UNMC).

A similar finding was noted in our prior audits.

During a review of users with Academic Institutional – Student Administration and Contributor Relations (SACR) security, 2 of 11 users tested had access that was not reasonable. One user was an employee at UNK, but had access to UNK and UNMC. The UNMC access was removed after this was brought to the attention of NeSIS staff. The other user had retired on May 29, 2015, but still had all of her roles, including update SACR access, as of June 11, 2015. These roles were removed after this was brought to the attention of NeSIS staff.

Also, during the review of user SACR security, it was noted there were three roles that allowed access to update SACR security. Thirty-three users, noted by campus below, had access to update SACR security.

Campus	# of Users
UNK	3
UNL	2
UNMC	17
UNO	2
UNCA	8
Consultants	1

After this was brought to the attention of NeSIS staff, two of the roles were changed to display only for SACR security. This left 16 users, noted by campus below, with access to update SACR security:

Campus	# of Users
UNK	2
UNL	1
UNMC	2
UNO	2
UNCA	8
Consultants	1

Designing powerful user roles with access across all campuses, without a way to track user activity, prevents accountability for user actions. Allowing update SACR access or update academic institution security to users who do not require this access as an essential part of their job duties increases the risk of unauthorized modifications made to the system. When access to networks and applications is not terminated timely, it creates the opportunity for unauthorized access to the system.

> We recommend the University review the design and use of the enrollment page role allowing update access across all campuses. We also recommend periodically reviewing users with the ability to update Academic Institutional SACR security to ensure only appropriate staff have access.

Management Response: *Access to the security roles described above has been removed for those end-users who do not need them. Each campus is permitted to determine which users should have the ability to update SACR Security. Queries can be run listing those users who have access to apply different levels of SACR security. These security reports are reviewed periodically by each campus security coordinator. The campuses have been asked to run and review the SACR security reports previously and will be reminded again this year. A NeSIS customization is pending review and approval which allow qualified users to check out the SACR update role but which will be removed at the end of the day.*

10. User Terminations

The University of Nebraska Executive Memorandum No.16 (Section 5) states the following:

> *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.*

InCommon Identity Assurance Profiles: Bronze & Silver (February 11, 2013), Section 4.2.4.2, states, "The IdPO shall revoke Credentials within 72 hours after being notified that a credential is no longer valid or is compromised." Human resource staff are responsible for notifying the Identity Provider Operator (IdPO) of terminations and should work to achieve access removal within a 72-hour period.

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

For 2 of 17 SAP terminated users tested, access was not removed within three business days. The time it took to remove access ranged from 4 to 18 business days and involved two UNMC employees.

A similar finding was noted in our prior audits.

For 15 of 24 NeSIS terminated users tested, access was not removed within three business days. The time it took to remove access ranged from 6 to 48 days. Seven of the 15 users logged into NeSIS subsequent to their termination date. The 15 users with access not removed timely included 7 at UNL, 2 at UNMC, and 6 at UNO. The seven users who logged into NeSIS subsequent to their termination date included two at UNL, one at UNMC, and four at UNO.

Additionally, it was noted UNL staff are notified of terminations twice a month when they receive a terminations report from SAP. The report is generally received on the first and third Monday of each month. This process would allow users to potentially retain access for more than two weeks after their termination date.

Failure to terminate user access timely creates the opportunity for unauthorized processing of transactions.

> We recommend the University implement a formal procedure at each campus to ensure the appropriate staff is notified of all terminations in order to remove NeSIS and SAP access within three business days and that this procedure be documented. We recommend the process include entering termination dates – when they are known – in SAP prior to the actual termination.

Management Response: *An enhanced Terminated User Report was completed in the fall of 2015 based on this past recommendation and is now used by the NeSIS security team and the campus NeSIS coordinators to assist them in de-provisioning NeSIS end-users. This daily report provides up to date information of HR actions pertaining to NeSIS business end-users, thus allowing improved, timelier information to determine when to remove NeSIS access.*

11. 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, prevention of student information databases from residing on mobile computing devices (including laptops, tablets, 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 a draft policy 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. However, the final version of the policy had not been completed.

A similar finding was noted in our prior audits.

A lack of policies and procedures for 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: *Policies around data governance and security are being subjected to a global review by the newly formed University Data Governance Council to ensure the privacy and protection of the data when it is extracted and downloaded by authorized users throughout the University.*

12. TrueYou and Mainframe Password Settings

The University's Password Policy, Version 1.1 (Revised March 4, 2014), states the following:

> *Any credential which identifies a subject or service account should follow recommendations outlined in National Institute of Standards (NIST) 800-63-2 [2], [3] using a token method and the level of entropy or randomness as outlined in §§ 6.1.2 and 6.3.*

National Institute of Standards and Technology (NIST) Special Publication 800-63-2 (August 2013), § 6.3.1.1, Electronic Authentication Guideline, presents token (password) requirements for various levels of assurance (LOA). Token requirements for LOA1 for pre-registered knowledge tokens state, "If the questions are not supplied by the user, the user shall select prompts from a set of at least five questions." An example of a question from a selected prompt could be, "What was your first pet's name?", with the answer becoming the pre-registered knowledge token. LOA1 requires a verifier to submit correct answers for at least three questions. Token requirements for LOA2 for pre-registered knowledge tokens state, "If the questions are not supplied by the user, the user shall select prompts from a set of at least seven questions." LOA2 requires a verifier to submit correct answers to at least five questions.

Good internal control includes system-enforced password parameters to ensure users meet minimum password standards. We noted the following during testing:

- The University's Identity Management system, known as TrueYou, is used for authenticating to SAP. UNK, UNL, and UNO also use TrueYou to authenticate to NeSIS. The TrueYou secondary authentication policy allows users to select prompts from a set of six questions and to reset their password by providing answers to only two of those questions, which are generated randomly. These parameters do not meet NIST standards.

- The mainframe Resource Access Control Facility (RACF) security settings include a set of password processing options. Passwords have a required length of eight characters, with at least one character having to be numeric. Mixed-case passwords are not supported, so all alpha characters are stored as uppercase. The limited character set of 39 and lack of complexity rules greatly reduce the level of password entropy or randomness.

> We recommend the University continue working to update system password parameters to meet policy, including minimum standards for pre-registered knowledge tokens. We also recommend reviewing the effects of changing RACF password processing options, and if practical, changing the options to support mixed-case passwords and changing the password syntax rules to 'mmmmmmmm,' requiring a password length of eight that must contain at least one alpha character, one lowercase alphabetic character, and one numeric character. Alpha characters are defined as uppercase alphabetic characters and the national characters #, $, and @.

Management Response: *Although the University considers the mainframe RACF observation as a low risk, we will review the TrueYou observation to determine the technical feasibility and password policy implications of this recommendation. Possible changes will permit RACF parameters to allow mixed case and special characters for use at logon password. TrueYou will be reviewed to determine the feasibility and impact of this recommendation.*

13. <u>SAP Security Access Controls</u>

The APA noted concerns regarding SAP logical security access. Due to the sensitive nature of the information in this comment, it has been disclosed to management in a separate communication.

Management Response: *The University acknowledges the concern expressed and has implemented security access controls to mitigate the associated risk.*

* * * * *

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 this management letter were furnished to the University administrators to provide them with an opportunity to review and respond to comments and recommendations contained herein. 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,

Mark Avery

Mark Avery, CPA
Audit Manager