The University of Nebraska

Management Letter

For the Year Ended June 30, 2016

Issued on February 3, 2017

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 9, 2016

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, 2016, and have issued our report thereon dated December 9, 2016.

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.

The following is a summary of our 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*. Our complete report can be found with our report on the financial statements of the University dated December 9, 2016.

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, 2016, 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 9, 2016. 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, the UNMC Science Research Fund, 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, the UNMC Science Research Fund, 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.*

We did note certain other matters that we reported to management included in the following Schedule of Findings and Responses.

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:

- UNL 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 UNL, 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 recorded in SAP agreed to the corresponding balances recorded in NeSIS. A redesigned process was initiated towards the end of the fiscal year but was not completed in a timely manner until after fiscal year end. This process will be evaluated by the auditor in the next audit. 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 $795,478 in SAP for the variance between SAP and NeSIS.

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.

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

A similar finding was noted in our prior audits.

> We recommend UNL 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.

Management Response: *The University understands the need to reconcile revenues and outstanding receivable balances. UNMC took measures to redesign the reconciliation for third party payments recorded in SAP and NeSIS shortly after fiscal year 2016 year end. UNL has developed new reconciliation procedures and reports to monitor and support the balances within NeSIS and SAP.*

2. <u>Audit Differences</u>

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 errors that resulted in significant misstatements. We proposed the University adjust its statements to correct all of these errors. The University did adjust the statements for all corrections proposed.

The following are significant misstatements the University corrected:

- A UNMC subsequent construction disbursement selected for testing, totaling $6,364,549, should have been accrued. Of that amount, $2,633,514 was properly accrued, but the remaining $3,731,035 was not properly accrued.
- UNL Chancellor's fees were recorded as expenditures for departments under the Office of Academic Affairs and revenue to the Chancellor's office. As this was transferring funds between departments within UNL, an eliminating entry should have been posted to avoid grossing up revenues and expenditures; however, no such entry was posted. This resulted in overstatements of Other Operating Revenue and Supplies & Materials Expense of $4,088,355. Additionally, a transfer of the balance in the Chancellor's Administrative fund to a new Cost Center was posted to the incorrect accounts and resulted in an overstatement of Other Operating Revenue of $4,067,490 and an understatement of Sales and Services of Educational Activities of $4,067,490.
- UNL did not properly record Othmer Fund income used to fund plant projects. This resulted in an understatement of Private Gifts of $5,858,201 and an overstatement of Capital Grants & Gifts of $5,858,201.
- UNL classified all $11,358,918 of its general fund accounts receivable as Sales and Services of Educational Activities on the Statement of Cash flows, but $5,547,572 was for accounts receivable related to tuition and fees. This resulted in Cash Inflows from Tuition and Fees being overstated by $5,547,572, and Increase in Cash Flows from Sales and Services of Educational Activities being understated by $5,547,572.

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.

A similar finding was noted in our prior audits.

> We recommend the University implement procedures to ensure financial information is complete, accurate, and in accordance with accounting standards.

Management Response: *It should be noted that the misstatements listed by the auditor have no impact on net position or net assets as reported. In our terminology, we call the items listed "reclassifications" as they move balances from one line item to another. We will re-examine the closing process to determine how to better capture reclassifications made at the campus level in preparing 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. 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, we noted several issues related to the UNO Dome contracting, billing, and receipting process.

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.

Neb. Rev. Stat. § 84-710 (Reissue 2014) states, in relevant part, the following:

> *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.*

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.

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

We noted the following issues related to the UNO Dome revenue entry selected for testing, comprised of six billings:

- One organization was under-billed on two separate invoices a combined 11 hours, at $200 per hour, for a total of $2,200 under-billed.

- Two receipts tested were not deposited timely in accordance with State statute. UNO received $1,600 from one organization and $800 from a separate organization on January 6, 2016. The receipts should have been deposited within three business days (by January 11, 2016) but were not deposited until January 20, 2016, which is six business days late.

- Three invoices tested did not include a payment due date (such as due within 30 days), which increases the risk UNO would be unaware of unpaid invoices.

A similar finding was noted in our prior audits.

> We recommend the University review the procedures for the UNO Dome and implement strong internal controls over the billing and collecting of revenues. We further recommend the legal department review the current contract template used by the UNO Dome. Additionally, we recommend invoices have due dates. We also recommend UNO implement procedures to ensure receipts are deposited timely in accordance with State statute. Finally, we recommend UNO implement procedures to review invoices to ensure organizations are billed properly.

Management Response: *UNO has made improvements to the fee sheet approval process and in documenting approval for any changes to contracts. The campus will continue to strengthen the internal controls as they relate to the billing and collection procedures.*

4. <u>Contracts not on the State Contracts Database</u>

During testing of 29 expenditures governed by contracts, 14 contracts and/or amendments were not included on the State Contract Database, as required by State statute. The contracts and/or amendments not included on the State Contract Database were 4 at UNL, 4 at UNK, 3 at UNMC, and 3 at UNO.

During the period audited, Neb. Rev. Stat. § 84-602.02(3)(a)(i) (Reissue 2014) provides 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[.]*

Due to the passage of legislation that became effective on July 21, 2016 – LB 694 (2016) and LB 851 (2016) – the above statutory provision has been transferred to Neb. Rev. Stat. § 84-602.04(4)(a)(i) (Reissue 2014). Though the language was also amended slightly, the University's duty thereunder remains unaltered.

A similar finding was noted in our prior audit.

> 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.*

5. General Ledger Transactions in SAP

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.

During our audit of the GL security roles in SAP, we identified 570 users with the ability to prepare and post GL entries in SAP without a system required secondary review or approval. The 570 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	316
UNMC	199
UNO	39
UNCA	12

(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	31
UNMC	23
UNO	12
UNCA	5

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

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.

When individuals are able to complete GL transactions without a system required secondary review or 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.

A similar finding was noted in our prior audits.

> 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 570 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 or 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.*

6. NeSIS Financial Aid Segregation of Duties

Nine users at UNCA 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 users were IT staff with a high level of access. In addition, six users (four at UNMC and two at UNL) had the ability to create a scholarship, configure the scholarship parameters, and then award that scholarship to a student in NeSIS.

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.

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.

A similar finding was noted in our prior audits.

> 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: *We agree with segregation of duties to achieve internal controls. The NeSIS Security Team will run a segregation of duties (SOD) role/permission audit report quarterly. End users identified with conflicting roles will be addressed either by removing security conflicts or requiring them to have a signed statement on file with the NeSIS security team, and the respective campus security coordinator, stating they accept the risks associated with the conflicting roles. The signed statements will be reviewed and updated annually. Campus SOD conflicts that continue after the quarterly reviews will be reported to the campus internal audit office for further review and resolution.*

Finally, several NeSIS support staff also have access to all FA roles which is required for problem resolution and for the application quarterly PeopleSoft maintenance. The NeSIS team is reviewing a solution to report all update activity by NeSIS staff and to log and document this required access.

7. NeSIS Improper Access

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 nine University users with this role (six UNO, two UNK, and one UNMC) had it for nearly four years.

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.

As of June 13, 2016, Computing Services Network (CSN) implemented a "Checkout Role" that allows select users temporary access to certain roles. The student records role is one of the roles that may be checked out by select users. APA confirmed on June 29, 2016, that no user was permanently assigned this role.

Designing powerful user roles with access across all campuses, without a way to track user activity, prevents accountability for user actions.

A similar finding was noted in our prior audits.

> We recommend the University review the design and use of the enrollment page role allowing update access across all campuses.

Management Response: *In August 2016, two NESIS system changes were completed and are in production to address this comment. The changes restrict end-user access to the enrollment page up to 24 hours after a specific documented or trouble shooting requirement is identified. If the assigned end-user does not check the role back in, a process is ran that checks the role back in and automatically de-activates it from the assigned end-user. The enrollment page access is also limited to a small number of authorized business end-users based on their position requirements after approval by the NeSIS Student Records Coordinator.*

8. User Terminations

For 3 of 30 SAP terminated users tested, access was not removed within three business days. The time it took to remove access ranged from five to seven business days and involved one UNK employee and two UNMC employees.

For 14 of 25 NeSIS terminated users tested, access was not removed within three business days. Of the 14 users with access not removed timely, 9 users had access removed between 4 and 27 business days after termination while 5 did not have access removed as of June 7, 2016. The 14 users with access not removed timely included 6 at UNL, 2 at UNMC, 2 at UNK, and 4 at UNO. The 5 users who did not have access removed as of June 7, 2016, included 1 at UNL, 2 at UNO, and 2 at UNMC. Additionally, 5 of the 14 users logged into NeSIS subsequent to their termination date. The 5 users who logged into NeSIS subsequent to their termination date included 2 at UNL, 2 at UNO, and 1 at UNK.

Additionally, it was noted that one other terminated employee still had NeSIS access after being terminated as of June 7, 2016. The employee was terminated on August 1, 2015.

It was noted also that 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 potentially allow users to retain access for more than two weeks after termination.

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 resources 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.

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

A similar finding was noted in our prior audits.

> 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 is documented. We recommend the process include entering termination dates – when they are known – in SAP prior to the actual termination.

Management Response: *Of the 14 NeSIS users referenced in the comment, all but one has been addressed and corrected. The remaining record is due to the individual retaining a 'volunteer' status. Future audit reports will include a report that not only analyzes the Terminated Date field, but also the Employee Group, which in the case of the remaining record is flagged as 'Active'.*

The Termination report is now available to the campuses daily in electronic form. An email notification is also sent to the campus security coordinators if there are new terminations allowing them to remove access in a timely manner.

9. NeSIS Data Extraction

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. The University is currently working on a project to classify data into various data risk classifications (i.e., high, medium, or low risk) but is yet to complete this project. No formal and approved policy is in place to document who extracts data, where the data is stored, and how the data is protected from security threats, though these processes are part of a Proposed Methodology document that is currently in draft form.

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.

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

A similar finding was noted in our prior audits.

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

Management Response: *The University Data Governance Council recommended policies and procedures for minimum security standards of campus and departmental servers and databases that contain high-risk, student information extracted from SAP and NeSIS. These standards will be followed and periodically monitored for compliance through the NU Security Council.*

10. TrueYou and Mainframe Password Settings

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; generated randomly. These parameters do not meet National Institute of Standards and Technology (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, where at least one character has to be numeric. The lack of complexity rules reduces the level of password entropy or randomness.

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.*

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.

The University of Nebraska Password Policy Technical Implementation Guide (effective December 31, 2013) states a user-chosen password should be "8 characters in length requiring upper, lower, and non-alpha characters" to meet NIST Level 1 (InCommon Bronze) or NIST Level 2 (InCommon Silver) standards for password entropy.

Good internal control includes system enforced password parameters to ensure users meet minimum password standards.

Inadequate password settings increase the risk of unauthorized users gaining access to sensitive information contained in both the NeSIS and SAP applications.

A similar finding was noted in our prior audit.

> We recommend the University ensure the password policy addresses the adequacy of not only passwords but also pre-registered knowledge tokens. We also recommend reviewing the effects of changing RACF password processing options and, if

practical, changing the password syntax rules to 'mmmmmmmm', requiring a password length of eight characters 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: *The TrueYou Identity Management System will be replaced in 2017 with a new, vendor based solution. During this replacement, the NIST password parameter requirements will be reviewed and changed as appropriate and possible within the new solution. Also, the RACF password rules were changed in January 2016 and include the use of mixed case and special characters.*

* * * * *

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 the 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