The University of Nebraska

Management Letter

For the Year Ended June 30, 2021

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 14, 2022

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
auditors.nebraska.gov

December 16, 2021

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, 2021, and have issued our report thereon dated December 16, 2021.

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 the knowledge of the University's organization gained during our work to make the following comments and recommendations, which 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 16, 2021.

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, fiduciary activities, and the discretely presented component unit of the University as of and for the year ended June 30, 2021, 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 16, 2021. 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 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), as described in our report on the University's financial statements. The financial statements of the Foundation and the Blended Component Units 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, which are 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. Audit Differences

During our audit of the financial statements of the University of Nebraska (University), we noted errors that resulted in significant ($1,000,000 or more) misstatements. We proposed the University adjust its financial statements to correct the identified misstatements. The University did adjust the financial statements for all proposed adjustments.

The following are the significant misstatements the University corrected:

- **Capital Expenditures in Accounts Payable:** The University improperly reflected capital expenditures in accounts payable (A/P) on the Statement of Cash Flows (SCF). The Auditor of Public Accounts (APA) noted that the University was reporting capital expenditures in accounts payable in the non-cash section of its SCF only for one of its component units. The APA brought this to the University's attention and questioned why the campuses and the University of Nebraska Central Administration System Office (UNCA) did not report this activity. Government Accounting Standards (GASB) Codification 2450.133 states, in relevant part, that in the noncash section of the SCF "[i]nformation about all investing, capital, and financing activities of a governmental enterprise during a period that affect recognized assets or liabilities but do not result in cash receipts or cash payments in the period should be reported." Following discussions with the APA, the campuses and UNCA ultimately added the following amounts of capital expenditures in A/P, by fiscal year end (FYE), as non-cash activity on the SCF:

  FYE June 30, 2021: $35,433,802
  FYE June 30, 2020: $26,041,741

  Additionally, the APA noted that the University improperly quantified cash outflows for purchases of capital assets and for payments to vendors on the SCF. UNL cash outflows for payments to vendors were overstated, and cash outflows for purchases of capital assets were understated by the following amounts, by fiscal year:

  FYE June 30, 2021: $3,230,799
  FYE June 30, 2020: $5,825,344

- **Group Health Program:** UNCA improperly reported activity for the University's group health insurance program (program) on the Statement of Revenues, Expenditures, and Change in Net Position (SRECNP) and the Statement of Changes in Fiduciary Net Position (SCFNP). UNCA reported the employer contribution portion for this program on the SRECNP and the employee contribution portion for this program on the SCFNP. It records year-end journal entries in its SAP accounting system to record program activity for the entire year based on how the activity is recorded on bank statements for the program. However, the APA expressed concerns that activity recorded in SAP did not agree to activity per the bank statements. UNCA looked into the APA's concern and determined that it had been netting together certain amounts when it prepared the SAP entries and would need to post adjusting entries to classify the activity properly. Based on a detailed review of program bank statements, UNCA determined the following amounts had been misclassified, by financial statement and by fiscal year:

FYE June 30, 2021 SRECNP

Line Item	Over (Under) Stated Amount
Compensation Expenses	$ (2,393,649)
Supplies and Services Expenses	$ (3,567,670)
Other Non-Operating Revenue	$ 3,521,868
Other Operating Revenue	$ (9,483,187)

FYE June 30, 2020 SRECNP

Line Item	Over (Under) Stated Amount
Compensation Expenses	$ (4,642,308)
Supplies and Services Expenses	$ (3,544,250)
Investment Income	$ 101
Other Operating Revenue	$ (8,186,659)

FYE June 30, 2021 SCFNP

Line Item	Over (Under) Stated Amount
Employer-Sponsored Cafeteria Plan Contributions	$ 808,279
Other Deductions	$ (1,111,579)
Employer-Sponsored Cafeteria Plan Deductions	$ 62,490
Other Additions	$ (1,857,368)

- **Fiduciary Statements:** University campuses were inconsistent in how (and if) they reported outside scholarship activity on the SCFNP. Initially, the University of Nebraska-Lincoln (UNL) did not include any outside scholarship activity on this statement, while the other three campuses did report such activity. Additionally, the University of Nebraska Omaha (UNO) reported certain types of student aid as outside scholarship activity on its SCFNP that was not actually outside scholarship activity; no other campus reported such activity on its SCFNP. The APA brought these discrepancies to the University's attention, and the campuses subsequently worked through their differences. UNL and UNO ultimately made the following adjustments to their SCFNPs:

  UNL: Added $7,388,433 in scholarship receipts
  Added $7,458,075 in scholarship expenses

  UNO: Removed $7,365,259 in scholarship receipts
  Removed $7,366,619 in scholarship expenses

- **HEERF Revenue Recognition:** UNL improperly reported Higher Education Emergency Relief Fund (HEERF) revenue and accounts receivable. HEERF includes both student aid and institutional portions. Based on guidance from the National Association of College and University Business Officers (NACUBO), the campuses reported HEERF institutional portion revenue based on the percentage of HEERF student portion funds they had expended. However, the APA noted that the percentage of HEERF institutional portion revenue UNL recognized during the fiscal year ended June 30, 2021, did not agree to the percentage of student portion funds it expended during the year. The APA brought this to UNL's attention, and it posted correcting entries to increase the amount of non-operating Federal grants and contracts revenue it recognized by $7,989,541, with an offsetting increase in the amount of accounts receivable it recognized.

- **Cash Flow Consolidation Error:** UNCA is responsible for consolidating stand-alone campus financial statements into University-wide financial statements. However, the APA noted that the amounts it recorded for University of Nebraska Kearney (UNK) cash flows did not agree to the amounts per UNK's stand-alone SCF. This resulted in cash inflows from gifts being overstated and cash inflows from Federal grants being understated by the following amounts, by fiscal year:

  FYE June 30, 2021: $5,828,000
  FYE June 30, 2020: $5,255,000

- **SRECNP Consolidation Error:** UNCA also improperly reflected a restatement it made to its own fiscal year ended June 30, 2020, SRECNP on the consolidated University-wide SCRENP. This resulted in other operating revenue being understated by $3,667,879 and compensation expenses being understated by the same amount.

- **Investment Cashflows:** UNCA failed to include all of its endowment investment purchases and sales activity on its SCF. This resulted in UNCA underreporting cash outflows for investment purchases by $3,021,040 and underreporting cash inflows for investment sales by $3,031,380.

- **Tuition Remissions:** UNL erroneously reported tuition remissions as prepaid expenses, which are included in "other assets" on the Statement of Net Position (SNP). This resulted in both unearned revenue and other assets being overstated by the following amounts, by fiscal year:

  FYE June 30, 2021: $1,556,148
  FYE June 30, 2020: $1,554,043

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 misstatements. Without such procedures, there is an increased risk that material misstatements may occur and remain undetected.

A similar finding was noted in our prior audits.

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

Management Response: The University strives to present financial statements accurately and in accordance with generally accepted accounting principles as prescribed by the Governmental Accounting Standards Board (GASB). We will continue to explore additional review processes, but there does not seem to be a significant return on the application of additional resources. We strive to perform an additional review step prior to providing draft statements to the APA.

2. 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 Automated Clearing House (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 506 users with the ability to prepare and post GL entries in SAP without a system-required secondary review or approval. The 506 users are noted by location below, along with the GL document types they could prepare and post:

Campus	# of Users
UNK	5
UNL	240
UNMC	206
UNO	32
UNCA	23

(Document Types: JE – Journal Entry, IB – Internal Charges Batch, and IC – Internal Charges Online)

A secondary role allowed 72 of those users to prepare and post additional GL document types. The 72 are noted by location below, along with the GL document types they could prepare and post:

Campus	# of Users
UNK	5
UNL	26
UNMC	16
UNO	12
UNCA	13

(Document Types: CN – ACH Receipt, ND – NIS Journal Entry, UU – University Only Journal Entry, UA – Accrual Journal Entry, TN – Interstate Billing Transaction, and PJ – Payroll Journal Entry)*

**NIS refers to the State's EnterpriseOne accounting system.*

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 of errors and inappropriate GL transactions occurring and remaining 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 for reviewing higher-risk GL 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 GL entries. Nevertheless, we continue to recommend that the University modify its role configuration for the 506 users identified, so 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: The University has previously conducted a cost/benefit analysis of implementing workflow within the SAP system to require review and approval of general ledger entries by a secondary approver. Given the significant estimated cost that would be required to implement workflow, we determined implementation is not justified at this time. We will continue our policy to review higher-risk general ledger transactions as a mitigating control.

3. <u>Contracts Not on the State Contracts Database</u>

During testing of 74 expenditures governed by contracts, 11 contracts and/or amendments were not included on the State Contracts Database, as required by State statute. The contracts and/or amendments not included on the State Contracts Database were seven at the University of Nebraska Medical Center (UNMC), three at UNL, and one at UNK.

Neb. Rev. Stat. § 84-602.04(4)(a)(i) (Cum. Supp. 2020) requires the Department of Administrative Services' web site to contain the following:

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 state entity, and by dollar amount. All state entities 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 . . . .

A similar finding was noted in our prior audits.

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

Management Response: The University will strive to continue filing contracts in the State Contracts Database on a timely basis. We are currently in the process of implementing a contract management system which we anticipate will improve our current process. Estimated go-live date is May 2022.

4. University Password Settings

The University's Identity Management system, known as SailPoint, is used for setting a global password policy. In addition, the University also establishes password settings and authenticates to SAP, the University's accounting system, through a central directory. UNK, UNL, and UNO also use the central active directory to authenticate to the Nebraska Student Information System (NeSIS). UNMC uses a separate active directory to authenticate to NeSIS.

During our review of the University's password settings in SailPoint and the central active directory, we noted the following settings were not in compliance with the National Institute of Standards and Technology (NIST) Digital Identity Guidelines:

- Users are allowed to select prompts from a set of six questions and to reset their password by providing answers to three of those questions, generated randomly.

- The University passwords that are stored in SailPoint were not salted and hashed, which are methods of encryption. The University's active directory is hashed but not salted.

- The University re-authentication settings for SAP and NeSIS were inadequate. Users were not required to re-authenticate to SAP and NeSIS until after 9 and 12 hours of inactivity, respectively.

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 outline in § § 6.1.2 and 6.3.

NIST has since issued Special Publication (SP) 800-63-3 in June 2017, which supersedes NIST SP 800-63-2. Additionally, SP 800-63-3, SP 800-63A, SP800-63B, and SP 800-63C provide technical guidance to agencies for the implementation of digital authentication.

NIST SP 800-63B (June 2017), § 5.1.1.2, states, in relevant part, the following:

Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.

* * * *

Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function. Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.

NIST SP 800-63B (June 2017), § 4.2.3, states, in relevant part, the following:

Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer. The session SHALL be terminated (i.e., logged out) when either of these time limits is reached.

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 audits.

> We recommend the University strengthen its password parameters to achieve compliance with NIST standards.

Management Response: The University of Nebraska has completed the rollout of two-factor authentication for all users to mitigate the risk of single-factor memorized secrets, and has removed the knowledge-based questions and answers for password reset. Users can currently reset their passwords with their NUID and a secondary or personal email account.

All passwords stored within the University Identity Management system are encrypted using industry standards, and this is needed to provision the multiple authentication stores for authentication. The University is working to consolidate authentication stores and once this is complete will be able to remove the encrypted passwords, leaving only the hashed passwords in the single store.

ITS will review the policy framework regarding the application session activity time-period taking into consideration the other management tools and security safe-guards in place against the risk.

5. User Terminations

For 4 of 25 terminated SAP users tested, access was not removed within three business days of the employees' last working date. The time it took to remove access ranged from 6 to 69 business days. The four users were all at UNL.

For 10 of 25 terminated NeSIS users tested, access was not removed within three business days of the employees' last working date. The time it took to remove access ranged from 6 to 751 business days. The 10 users included one at the Institute of Agriculture and Natural Resources (IANR), two at UNK, four at UNL, and three at UNO.

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.

The University of Nebraska Executive Memorandum No. 26 ("Information Systems" section) states, in relevant part, the following: "Access to covered data and information via the University's computer information system is limited to those employees who have a business reason to know such information."

InCommon Identity Assurance Profiles: Bronze & Silver (February 11, 2013), Section 4.2.4.2, states, "The IdPO [Identity Provider] 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 IdPO of terminations and should work to achieve access removal within a 72-hour period.

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

> We recommend the University implement a formal procedure at each campus to ensure the appropriate staff is notified timely of all terminations of SAP and NeSIS users, thereby facilitating removal of access to those systems within three business days. The notification and removal processes should be properly documented. We also recommend such process include entering termination dates – when they are known – in SAP prior to the actual terminations.

Management Response: A committee was formed to review the business practices, procedures and policies. The recommendations of the committee were presented and some actions were taken to address this issue.

Our SAP system has an automated process that removes all backend access to non-self-serve applications related to the employee after a separation action date is processed. Thirty days from the separation date all access is removed from each separated employee. In the last year, as part of the above mentioned committee's recommendation, a new daily report is shared with the campuses that shows the employee separation action date versus last working date. In addition, the report shows the number of days late the entry date is compared to the last working date. Finally, a report is provided to the Senior Vice President | CFO of any separation that exceeds 5 days (biweekly) or 20 days (monthly). The CFO requires the campus chief business officer to provide an explanation on why the exception occurred.

NeSIS has a scheduled report delivered to the NeSIS campus security coordinators each business day which is cumulative and shows any user who is assigned roles giving access to data or pages outside the dashboard/selfservice or guest access when that user is no longer employed. This report is also available to run adhoc.

* * * * *

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 they 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 suitable for any other purpose. However, this communication is a matter of public record, and its distribution is not limited.

Sincerely,

Mark Avery

Mark Avery, CPA
Assistant Deputy Auditor