The University of Nebraska

Management Letter

For the Year Ended June 30, 2022

Issued on February 13, 2023

NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

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

December 16, 2022

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, 2022, and have issued our report thereon dated December 16, 2022.

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, 2022.

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, 2022, 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, 2022. 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 the results of the other auditors' testing of internal control over financial reporting or compliance and other matters that are reported on separately by those auditors.

Report on 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.

Report on Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of 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. Financial Statement Errors

During our audit of the financial statements of the University of Nebraska (University), we noted errors that resulted in significant 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:

- **Net Investment in Capital Assets**: The University overstated its net investment in capital assets by $50,756,376 and $31,856,400 for the fiscal years ended June 30, 2022, and June 30, 2021, respectively. Per guidance from the Government Finance Officers Association (GFOA) and Governmental Accounting Standards Board (GASB), this net position classification should be calculated net of fiscal-year-end capital-related accounts payable and retainages payable. However, the University included these payables in other net position categories, leading to the following misstatements of net position amounts on its Statement of Net Position (SNP), by fiscal year:

Fiscal Year 2022

Net Position Category	Over (Under) Stated Amount
Invested in Capital Assets, Net of Related Debt	$ 50,756,376
Externally Restricted Funds	$ (1,313,270)
Plant Construction	$ (45,562,257)
Unrestricted	$ (3,880,849)

Fiscal Year 2021

Net Position Category	Over (Under) Stated Amount
Invested in Capital Assets, Net of Related Debt	$ 31,856,400
Externally Restricted Funds	$ (1,242,943)
Plant Construction	$ (26,965,101)
Unrestricted	$ (3,648,356)

- **UNO Capital Asset Entry**: During fiscal year 2022, the University of Nebraska Omaha (UNO) had additional costs on a building it previously capitalized. To add the additional costs, the campus first posted an entry to remove the carrying value previously recorded for the building and then posted an entry to re-add the asset with the additional costs included. The entry to remove the asset resulted in recording of revenues and expenses in the University's accounting system that are not true University revenues and expenses. This activity should be eliminated; however, when preparing its financial statements, UNO did not remove this activity, resulting in UNO overstating both revenue and supplies and services expenses by $36,837,834.

- **UNOP Statement of Cash Flows (SCF)**: During our review of the SCF the University of Nebraska Office of the President (UNOP) prepared, we noted the following:

  - UNOP improperly classified $29,977,139 in cash inflows for fiscal year 2021 and $16,664,250 in cash outflows for fiscal year 2022. The activity was associated with the University's Imprest Payroll Fund, which the University uses to process payroll expenses. UNOP reported this activity as cash inflows for other receipts when it should have reported it as cash outflows for payments to employees.

- During the fiscal year 2022, the University implemented GASB Statement No 87, *Leases*, and restated its fiscal year 2021 financial statements for comparability. However, UNOP and the campuses were inconsistent in what lease activity they reported as non-cash acquisition of right-to-use assets through lease obligation transactions on their restated fiscal year 2021 SCFs. The campuses reported only leases entered into during the fiscal year on this line, while UNOP reported all leases it recognized for the first time on its balance sheet in connection with its initial adoption of GASB 87. After the APA brought this inconsistency to UNOP's attention, it reduced the amount it reported by $8,813,288.

- The ending cash balance UNOP reported as of June 30, 2021, on its SCF was $3,811,404 greater than the amount it reported on its SNP. It reduced cash activity reported on various SCF line items to correct this error.

- **UNMC Building Retirements**: The University of Nebraska Medical Center (UNMC) did not properly account for building retirements when it determined its beginning net position and depreciation expenses for fiscal year 2022. UNMC ultimately made correcting entries for the following errors on its SNP and Statement of Revenues, Expenditures, and Changes in Net Position (SRECNP):

Line Item	Financial Statement	Over (Under) Stated Amount
Capital Assets Net of Accumulated Depreciation	SNP	$ (11,077,314)
Beginning Fund Balance	SRECNP	$ 9,658,642
Depreciation Expense	SRECNP	$ 11,209,914
Supplies and Services Expenses	SRECNP	$ 9,486,765
Other Non-Operating Revenue (Expenses)	SRECNP	$ 39,277

- **Component Unit Cash Flows**: UNOP is responsible for consolidating stand-alone University campus and component unit financial statements into the University-wide financial statements. When UNOP blended in cash flow activity for one of the University's component units, it improperly reported $19,092,000 in fiscal year 2022 non-cash transactions for capital expenditures in accounts payable for the component unit. The amount per the component unit's audited financial statements was $26,599,000, an audit difference of $7,507,000.

- **UNO Cash Flows**: The amount UNO reported as fiscal year 2022 non-cash capital expenditures in accounts payable transactions on its SCF included $3,795,000 in transactions that occurred during the prior fiscal year and that it also reported as non-transactions for fiscal year 2021.

- **UNL Deferred Inflows**: The University of Nebraska Lincoln (UNL) improperly calculated deferred inflows associated with its service concession arrangements, resulting in it overstating the amounts it reported as deferred inflows and accounts receivable by $1,496,475.

- **UNMC Investment Income**: UNMC misclassified $1,277,380 in investment income as revenue from an increase in investment fair market value revenue.

- **Fiduciary Statements:** During our review of the University's fiduciary activity statements, we noted the following:

  - The Nebraska Statewide Workforce & Educational Reporting System (NSWERS) is a fiduciary component unit of the University. UNOP improperly reported cash balances (and associated activity) held and reported by the University of Nebraska Foundation, a discrete component unit of the University, on its fiduciary activity statements. This resulted in various misstatements, including a $2,304,000 overstatement of the amount it reported as fiduciary cash.

- UNL has control of funds for the Nebraska Council of Economic Education (NCEE). The campus reported NCEE activity on its business-type activity statements. However, given that the NCEE is legally separate from the University, the APA questioned whether this presentation was appropriate. Following APA inquiry, UNL reclassified the activity, including $262,668 in additions and $267,296 in deductions, from business-type to fiduciary-type activity.

- UNL double recorded $126,740 in student fee revenue (and offsetting cash) as both business-type revenue and fiduciary-type additions. As this is UNL's revenue, it should not have been reported on the campus's fiduciary-type statements.

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 the cost/benefit return of increasing resources to implement additional review processes.

2. General Ledger Transactions in SAP

The workflow in the SAP, the University's accounting 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 507 users with the ability to prepare and post GL entries in SAP without a system-required secondary review or approval. The 507 users are noted by location below, along with the GL document types they could prepare and post:

Campus	# of Users
UNK	5
UNL	243
UNMC	202
UNO	32
UNOP	25

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

A secondary role allowed 79 of those users to prepare and post additional GL document types. The 79 users are noted by location below, along with the GL document types they could prepare and post:

Campus	# of Users
UNK	5
UNL	31
UNMC	18
UNO	14
UNOP	11

(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 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 507 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: While the University believes it's current review process of general ledger transactions does mitigate risk, we agree that having a workflow approval within SAP for general ledger entries is a sound business practice. Therefore, we plan to implement approval workflow within SAP. As discussions regarding the implementation are just beginning, we do not yet have an anticipated completion date. However, this will be a high priority project.

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

During testing of 42 expenditures governed by contracts, 12 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 UNMC, two at UNL, and three at UNO.

Neb. Rev. Stat. § 84-602.04(4)(a)(i) (Cum. Supp. 2022) 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 strives to file contracts in the State Contracts Database on a timely basis. We continue to evaluate our current upload process to identify opportunities for improvement.

4. <u>University Password Settings</u>

The University's Identity Management system is used for setting a global password policy. In addition, the University establishes password settings and authenticates to the Nebraska Student Information System (NeSIS) and to SAP through various active directories.

During our review of the University's password settings, we noted that all authenticators used to access NeSIS and SAP were not salted and hashed, as required by the National Institute of Standards and Technology (NIST) Digital Identity Guidelines.

Additionally, during testing of reauthentication settings, we noted that not all users are required to reauthenticate to SAP and NeSIS within the limits established by NIST guidelines.

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. The University is in the process of developing a new policy for access, identification, and authentication standards; however, as of testing, it was still in draft status.

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

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 has 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 published an updated Access, Identification, and Authentication Standard (ITS-02), including the requirement of two-factor authentication for all users to mitigate the risk of single-factor memorized secrets.

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 salted and 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. Our approach will be to strive for a more restrictive session timeout setting for administrative access and a less restrictive setting for a student or someone with limited access.

5. User Terminations

For 4 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 71 business days. The four users included two at UNO, one at UNL, and one at UNK.

For 2 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 9 business days. The two users were both at UNL.

Additionally, during our review of University employees with access to EnterpriseOne (E1), the State's accounting system, we noted two terminated employees who had access to E1. Following APA inquiry, the access was removed. The time it took to remove access ranged from 23 to 45 business days. The two users included one at UNL and one at UNMC.

Section 5 of University of Nebraska Executive Memorandum No. 16 ("Policy for Responsible Use of University Computers and Information Systems") (Revised May 11, 2022) states the following:

> *Unauthorized access to Information Systems is prohibited . . . . As individuals' relationships with the University change or terminate, their authorized access to systems, services, and data shall be adjusted in accordance with Board of Regents or other University polices.*

The "Information Systems" section of University of Nebraska Executive Memorandum No. 26 ("University of Nebraska Information Security Plan") (September 9, 2014) 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 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 (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 support that such access was properly removed.

> We recommend the University strengthen procedures to ensure the appropriate staff is notified timely of all terminations of NeSIS, SAP, and E1 users, thereby facilitating removal of access to those systems within three business days. The notification and removal process should be properly documented.

Management Response: 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. A 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/self-service or guest access when that user is no longer employed. This report is also available to run ad hoc.

Currently, El terminations must be communicated to Business & Finance from the campuses. We will work with the NeBIS team to automate an email notification to Business & Finance when an employee with El access separates.

6. Accounts Payable (A/P) Transactions

During our audit of the A/P security roles in SAP, we noted that six users had the ability to prepare an invoice, post it in SAP, and also approve and post it in E1. Additionally, two of the six users had the ability to create a purchase order, prepare the invoice related to the purchase order, and post the transaction in both SAP and E1. Finally, three of the six users could set up a vendor in SAP.

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

A good internal control plan requires a proper segregation of duties to ensure that 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.

A lack of segregation of duties in the A/P process allows a single individual to make purchases and pay vendors without a secondary review or approval. Additionally, some of those users had the ability to create new vendor records in SAP. This risk allows for the possible theft or misuse of State funds.

> We recommend the University review the security design of the A/P roles in SAP and implement controls that require separate individuals to prepare and post A/P transaction types. We also recommend reviewing users with the ability to create vendors in SAP to ensure a proper segregation of duties exists.

Management Response: The University is in process of implementing a tool which will identify potential segregation of duties conflicts within all security roles in SAP at the point of role assignment. Existing role assignments will also be evaluated and any current conflicts addressed during implementation.

* * * * *

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 intended to be, and should not be, used by anyone other than these specified parties.

Sincerely,

Mark Avery, CPA
Assistant Deputy Auditor