MANAGEMENT LETTER
OF THE
NEBRASKA STATE COLLEGE SYSTEM

For the Year Ended June 30, 2021

Issued on December 29, 2021

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

Mr. Paul Turman, Chancellor
Board of Trustees
Nebraska State College System
1327 H Street, Suite 200
Lincoln, Nebraska 68508-3751

Dear Mr. Turman:

We have audited the financial statements of the Nebraska State College System (NSCS) (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 our knowledge of the NSCS'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 Nebraska State College System dated December 16, 2021.

We have audited in accordance with 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 units of the NSCS, as of and for the year ended June 30, 2021, and the related notes to the financial statements, which collectively comprise the NSCS'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 Nebraska State College System Foundations, the Nebraska State Colleges Facilities Corporation, and the activity of the Nebraska State College System Revenue and Refunding Bond Program, as described in our report on the NSCS's financial statements. The financial statements of these entities and program 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 NSCS'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 NSCS's internal control. Accordingly, we do not express an opinion on the effectiveness of the NSCS'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 NSCS's financial statements will not be prevented, or detected and corrected, on a timely basis. A *significant deficiency* is a deficiency or combination of deficiencies in internal control that is less severe than a material weakness, yet important enough to merit attention by those 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 NSCS'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.*

Nebraska State College System's Response to Findings

We did note certain other matters that we reported to management of the NSCS, which are included below. The NSCS's responses to our findings are described below. The NSCS's responses were not subjected to the auditing procedures applied in the audit of the financial statements; accordingly, we express no opinion on them.

Comment No. 2021-001: Financial Statement Errors

During our audit of the financial statements of the Nebraska State College System (NSCS), we noted errors that resulted in significant misstatements. We proposed the NSCS adjust its financial statement to correct the identified misstatements. The NSCS did adjust the financial statements for all proposed adjustments.

The following are the significant misstatements the NSCS corrected:

- Wayne State College (WSC) recorded an entry for work completed on the Energy Plant Upgrades project and paid by the Nebraska Department of Administrative Services (DAS) through the LB 309 Task Force in July 2021 as a fiscal year 2022 activity. However, the expense was for work completed in June 2021 and should be accrued in fiscal year 2021. This caused both the Capital Assets and Capital Appropriations and Grants revenue to be understated by $271,427.

- Peru State College (PSC) records expenditures and revenues related to processing alternative loan activity. Alternative loans are private loans obtained by a student through a financial institution that verifies the student's status with the college and remits the loan funds to the college for application to the student's account. As the college does not have an administrative role in this process, this would be considered pass-through activity and should be eliminated from the financial statements. In preparing the PSC financial statements, PSC did not eliminate alternative loan activity, which resulted in Private Grants and Contracts revenue being overstated by $221,724 and $182,816 in fiscal years 2021 and 2020, respectively, and Scholarships and Fellowships expense being overstated by $229,179 and $176,328 in fiscal years 2021 and 2020, respectively.

- When preparing the Statement of Cash Flows for fiscal year 2020, Chadron State College (CSC) incorrectly recorded $412,781 of equipment paid by DAS through the Master Lease program as cash inflows and cash outflows. This caused cash flows for Payments to Suppliers to be overstated by $412,781 and cash flows from Non-Capital Financing Other Receipts to be overstated by $412,781. Additionally, CSC made a purchase of $43,002 of capital assets through the Master Lease program, which was paid for by CSC and reimbursed by DAS. This payment was incorrectly recorded as a cash flow from Non-Capital Financing Other Receipts, causing cash flows from Non-Capital Financing Other Receipts to be overstated by $43,002 while cash flows from Capital Financing Other Receipts was understated by $43,002.

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

A similar finding has been noted since the fiscal year 2016 audit; however, the Nebraska Auditor of Public Accounts has noted significant improvement in procedures related to the preparation of the financial statements, resulting in a decrease in the number of significant misstatements identified.

> While the NSCS has improved procedures related to the preparation of its financial statements, we recommend the NSCS continue to strengthen procedures to ensure internally prepared information is complete and accurate upon submission to the auditors.

NSCS's Response: The NSCS understands that accuracy of the financial statements is important. The NSCS remains committed to finding ways to continue to improve on existing procedures for the financial statement preparation and review process prior to submission to reduce financial statement errors.

Comment No. 2021-002: Password Settings

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

During our review of the NSCS 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 passwords by providing answers to three of those questions, generated randomly.

- NSCS passwords that are stored in SailPoint were neither salted nor hashed, which are methods of encryption. The passwords stored in the central active directory were hashed but not salted.

During our review of CSC's password settings in its active directory, we noted the following settings were not in compliance with NIST Digital Identity Guidelines:

- The passwords that are stored in the active directory were hashed but not salted.

- Passwords are not checked against a list that contains values known to be commonly used, expected, or compromised.

During our review of WSC's password settings in its active directory, we noted the following settings were not in compliance with NIST Digital Identity Guidelines:

- The passwords that are stored in the active directory were hashed but not salted.

University of Nebraska (University) staff manage the SAP and NeSIS applications on behalf of both the University and the NSCS. 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 has since issued Special Publication (SP) 800-63-3 in June 2017, which supersedes NIST SP 800-63-2. Along with SP 800-63-3, SP 800-63A, SP 800-63B, and SP 800-63C provide technical guidelines 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.*
>
> * * * *
>
> *When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised.*

* * * *

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.

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 has been noted since the fiscal year 2011 audit.

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

NSCS's Response: The University of Nebraska and Nebraska State College System continue to expand adoption of two-factor authentication to mitigate the risk of single-factor memorized secrets. The University has a revised password policy that aligns with the latest recommendations in NIST 800-63-3, which is currently in the process of ratifying with stakeholders.

Chadron and Wayne State College acknowledges the comment and notes that Microsoft Active Directory on premise is not capable of salting passwords. If and when Microsoft develops these capabilities, CSC and WSC will implement them. Additionally, effective August 10, 2021, CSC moved to the Microsoft Password Manager service that checks password dictionaries maintained by Microsoft, as well as allows CSC to disallow passwords they specify.

Comment No. 2021-003: 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 NSCS could complete GL transactions from beginning to end without a documented secondary review and approval in SAP. Each NSCS location (the three Colleges and the System Office) developed its own unique compensating controls to address this inherent system weakness. However, in general, the compensating controls put in place at all NSCS locations included a manual documentation of the preparer and poster of the GL transactions.

During our audit of the GL security roles in SAP, we identified 26 users with the ability to prepare and post GL entries in SAP without a secondary, system-required review or approval. The 26 users are noted by location below, along with the GL document types they could prepare and post:

Location	# of Users
Wayne State College (WSC)	7
Peru State College (PSC)	6
Chadron State College (CSC)	6
NSCS System Office	5
UNCA (University)	2

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

A secondary role allowed all 26 of those users to prepare and post additional GL document types. The 26 users capable of preparing and posting additional GL document types without a secondary, system-required review or approval are noted by location below, along with the GL document types they could prepare and post:

Location	# of Users
WSC	7
PSC	6
CSC	6
NSCS System Office	5
UNCA (University)	2

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

**NIS refers to the State's EnterpriseOne accounting system.*
***Role is used for College Only Journal Entries; however, the document type is also used by the University of Nebraska, which shares the SAP environment with the State Colleges.*

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.

When individuals are able to complete GL transactions without a system-required, documented, secondary review and approval prior to posting the transaction to the GL, there is a greater risk for error and for 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 has been noted since the fiscal year 2014 audit.

> We recognize that the NSCS has worked to implement compensating controls to mitigate the risks related to the SAP system's lack of 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 NSCS work on a system-based SAP solution as well.

NSCS's Response: The Colleges review the users' access annually and determines if current access is necessary based on how the roles are defined within SAP. As noted above by the auditors, the NSCS has compensating controls in place.

Comment No. 2021-004: Accounts Payable (A/P) Transactions

During our audit of the A/P security roles in SAP, the NSCS's accounting system, we noted that eight users had the ability to prepare an invoice, post it in SAP, and also approve and post it in EnterpriseOne (E1), the State's accounting system. Additionally, two of the eight 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, six of the eight users could set up a vendor in SAP.

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

Location	# of Users
Chadron State College (CSC)	2
Peru State College (PSC)	3
Wayne State College (WSC)	1
NSCS System Office	2

Two of the eight users identified above could also prepare a purchase order, as noted by location below:

Location	# of Users
CSC	0
PSC	0
WSC	0
NSCS System Office	2

Six of the eight users identified above could also set up a vendor in SAP, as noted by location below:

Location	# of Users
CSC	2
PSC	2
WSC	0
NSCS System Office	2

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 and misuse of State funds.

A similar finding has been noted since the fiscal year 2014 audit.

> We recommend the NSCS 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.

NSCS's Response: The Colleges review the SAP and EnterpriseOne users' access for all accounting staff annually and make changes as necessary to ensure adequate daily operations while still striving to meet best practices for internal control. The NSCS agrees that this deserves continued efforts and will continue to seek solutions that will further diminish risk and take into account the NSCS's small operating staff.

* * * * * *

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

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

This letter is intended solely for the information and use of NSCS management, the Board of Trustees, others within the NSCS, and the appropriate Federal and regulatory awarding agencies and pass-through entities, and it is not suitable for any other purpose. However, this letter is a matter of public record, and its distribution is not limited.

Sincerely,

Zachary Wells, CPA, CISA
Audit Manager