MANAGEMENT LETTER
OF THE
NEBRASKA STATE COLLEGE SYSTEM

For the Year Ended June 30, 2020

Issued on December 18, 2020

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 14, 2020

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, 2020, and have issued our report thereon dated December 14, 2020.

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 14, 2020.

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, 2020, 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 14, 2020. 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. 2020-001: 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 statements 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:

- Peru State College (PSC) received $379,836 in institutional aid from the Coronavirus Aid, Relief, and Economic Security (CARES) Act to cover costs associated with significant changes to the delivery of instruction due to the COVID-19 pandemic. When preparing its financial statements, however, an adjusting entry was not performed to eliminate a $379,836 overstatement of Federal Grants and Contracts revenue and Scholarships and Fellowships expense resulting from the process of recording and receipting the CARES Act revenue in the SAP System (NSCS's accounting system).

- When preparing the Statement of Cash Flows, PSC adjusted the cash outflows for Payments to Suppliers to remove expenses for account write-offs, which have no cash outflow. However, PSC used the amount for Bad Debt Expense from the trial balance rather than actual write-offs. This caused the cash outflows from Payments to Suppliers to be overstated by $102,076, Tuition and Fees Receipts to be overstated by $21,797, and Sales and Services of Auxiliary Enterprises Receipts to be overstated by $80,279.

- When calculating the classification of Net Position, PSC used the incorrect amount for monies Restricted by Enabling Legislation due to an adjustment for the Revenue Bond audit completed after the preparation of the financial statements. This caused Net Position – Other to be understated by $373,550 and Net Position – Unrestricted to be overstated by $373,550.

- An increase in Other Receivables was recorded incorrectly to Other Receipts (Payments) from Non-Capital Financing Activities on the Statement of Cash Flows. This caused Grants and Contracts Receipts from Operating Activities to be understated by $4,882, Other Receipts (Payments) from Non-Capital Financing Activities to have payments overstated by $245,729, Payments to Suppliers to be understated by $71,857, Payments to Employees to be understated by $16,753, Other Payments from Operating Activities to be understated by $37,430, and Grants and Contracts Receipts from Non-Capital Financing Activities to be overstated by $124,571.

- When calculating the classification of Net Position, Chadron State College (CSC) erroneously did not include $1,174,064 in its calculation of Net Position – Restricted for Plant. This caused Net Position – Restricted for Plant to be understated by $1,174,064, Net Position – Unrestricted to be overstated by $1,174,030, and Net Position – Restricted for Other to be overstated by $34.

- Additionally, PSC erroneously expensed $288,281 of retainage for the Theatre renovation on the financial statements for the period ending June 30, 2019. This error was due to a payable for retainage on construction that should have been capitalized. As a result, Supplies, Materials, and Other Expense were overstated and Capital Assets were understated by $288,281.

A good internal control plan and sound accounting practices require financial information to be complete and accurate. This includes procedures to ensure that financial statements are correct and any needed 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. The fiscal year 2017 finding was a material weakness. The fiscal year 2018 finding was a significant deficiency. The fiscal year 2019 finding was not as severe as those of the two prior years, but the APA had a reportable comment nonetheless.

> We recommend the NSCS 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 Colleges experienced higher than normal employee leave and turnover throughout the FY20 audit, however 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. 2020-002: Other Operating Revenue Issues

During testing of 15 Other Operating Revenues transactions, the APA noted issues with receipts lacking adequate support, receipts not being deposited timely, and coding not being performed properly. These issues are described in more detail below:

For four transactions tested, adequate supporting documentation was not available. Information about the four transactions is provided below:

1. CSC entered into a Food Service Partnership Agreement with a third party. According to that agreement, the third party is required to provide concession service at all athletic events, and sales are to be deposited by the College Athletic Department; however, CSC lacked adequate procedures for ensuring that concession sales received were accurate and complete.

2. A $13 receipt at WSC had no order form on file; therefore, the APA was unable to determine if the correct amount was received.

3. A $10,870 PSC deposit for athletic camps included $2,350 in cash receipts; however, PSC lacked documentation to support that two individuals were involved in the receipting process.

4. A $3,106 WSC deposit for a band program included $411 in cash receipts; however, WSC lacked documentation to support that two individuals were involved in the receipting process. Included in the $411 cash receipts was $396 in band program admissions for which WSC lacked documentation to support that this was the proper amount to be deposited.

For six transactions tested, cash and checks received were not deposited in a timely manner, as noted below:

1. A $6,631 CSC deposit made on February 20, 2020, included cash and checks received between January 9, 2020, and February 17, 2020. Of the $6,631 deposited, $6,451 was not deposited within three business days, as required by statute. Additionally, two receipts, totaling $30, did not have a date received documented, so the APA was unable to determine if they were deposited timely.

2. An $8,700 CSC deposit made on December 9, 2019, was for concession sales at sporting events from November 8, 2019, to December 1, 2019. CSC received the funds from a third party vendor on December 2, 2019. None of these receipts were deposited within three business days, as required by statute.

3. A $25,000 CSC corporate sponsorship deposit was deposited four business days after it was received.

4. A $2,012 PSC deposit for football gate sales was deposited four business days after it was received.

5. A $10,870 PSC deposit included checks and cash for football and basketball summer camps received between July 8, 2019, and July 18, 2019; however, these amounts were not deposited until July 24, 2019, which did not comply with statute.

6. A $16,539 PSC deposit included checks received on March 18, 2020, and March 20, 2020, that were not deposited until March 26, 2020, which is after the three business days required by statute.

For two transactions tested, issues were noted with how the revenues were being recorded in the accounting system.

1. For athletic gate receipts, PSC records sales tax separately from ticket sales for tracking purposes; however, one $2,012 ticket sales deposit included $123 of sales taxes recorded as football revenue.

2. One WSC athletic gate receipt was overstated by $10 because a refund was processed during the game, but it was not reflected on the transmittal.

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.*

A good internal control plan requires procedures to ensure that funds received are for the correct amounts, agree to adequate supporting documentation, and are deposited timely. Those same procedures should ensure also that there is a documented segregation of duties when collecting monies. Without such procedures, there is an increased risk for the loss of revenues.

Similar findings were noted in the prior three audit reports.

> We recommend the NSCS implement procedures to ensure there is an adequate segregation of duties over the receipting of cash, receipts are deposited in a timely manner in compliance with State statute, and adequate supporting documentation is obtained and kept on file to ensure amounts received are for the correct amount and properly recorded.

NSCS's Response: The NSCS continues to look for ways to improve the documentation associated with revenue collections. Some of the items noted are minimal and the risk of lost revenue may not warrant the cost of additional staff. The Colleges will review each area and continue to work with the departments and their revenue collection procedures.

Comment No. 2020-003: Password Settings

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

During our review of the State Colleges' 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 State Colleges passwords that are stored in SailPoint were neither salted nor hashed, which are methods of encryption. The passwords 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 were stored at the active directory were hashed but not salted.

- The required minimum password length for staff and students was only seven characters.

- Staff and student users did not have their accounts locked after multiple consecutive failed authentication attempts.

- Passwords were 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 were stored at the eDirectory were neither salted nor hashed.

- The passwords that were stored on WSC's 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 State Colleges. 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:

> *Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters in length.*
>
> * * * *
>
> *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 implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as describe in Section 5.2.2.*
>
> * * * *
>
> *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), § 5.2.2., states, in relevant part, the following:

> *Unless otherwise specified in the description of a given authenticator, the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.*

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 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. Dictionary checks for passwords within the SailPoint system have also been implemented.

The CSC Active Directory base password policy was changed to 10 characters on 10/05/2020, and the Account Lockout in Active Directory was set to 15 attempts on 10/12/2020. A Password Dictionary upgrade is in the process of evaluation, and implementation is anticipated in the current fiscal year.

Wayne State College acknowledges the comments and has priority plans underway to decommission eDirectory, which then allows the College to enhance passwords salting in Active Directory. This work should be completed within the next few months.

Comment No. 2020-004: 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 22 users with the ability to prepare and post GL entries in SAP without a secondary, system-required review or approval. The 22 users are noted by location below, along with the GL document types they could prepare and post:

Location	# of Users
Wayne State College (WSC)	8
Peru State College (PSC)	4
Chadron State College (CSC)	5
NSCS System Office	3
UNCA (University)	2

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

A secondary role allowed 21 of those users to prepare and post additional GL document types. The 21 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	8
PSC	4
CSC	4
NSCS System Office	3
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 determine 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.

<u>Comment No. 2020-005: Accounts Payable (A/P) Transactions</u>

During our audit of the A/P security roles in SAP, we noted that 10 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, 4 of the 10 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, 8 of the 10 users could set up a vendor in SAP.

The 10 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)	4
Wayne State College (WSC)	1
NSCS System Office	3

Four of 10 users identified above could also prepare a purchase order, as noted by location below:

Location	# of Users
CSC	1
PSC	0
WSC	0
NSCS System Office	3

Eight of the 10 users identified above could also set up a vendor in SAP, as noted by location below:

Location	# of Users
CSC	2
PSC	3
WSC	0
NSCS System Office	3

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.

<u>Comment No. 2020-006: NeSIS User Termination</u>

For 5 of 11 NeSIS terminated 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 7 to 170 business days. The five users included three at PSC and two at WSC.

The Nebraska State College Policy 5008 (January 24, 2020), Employee Use of System Technology Resources, states the following:

> *When any employee terminates his or her employment with the College or System Office, his or her credentials shall be denied further access to Technology Resources unless otherwise determined by the President or Chancellor.*

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 indicate that such access was properly removed.

> We recommend the NSCS implement a formal procedure at each College to ensure the appropriate staff is notified of all terminations in order to remove NeSIS access within three business days and that this procedure be documented.

NSCS's Response: A new report was created to identify separation actions that are entered beyond three days after the separation date. Colleges will use this report for identifying situations that fall outside of the parameters and take further steps to ensuring timely separations, if necessary.

* * * * * *

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

Sincerely,

Zachary Wells

Zachary Wells, CPA, CISA
Audit Manager