CHRISTOPHER NEWPORT UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2019

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of Christopher Newport University as of and for the year ended June 30, 2019, and issued our report thereon, dated May 15, 2020. Our report is included in the University's Financial Statements that it anticipates releasing on or around June 15, 2020. Our audit found:

- the financial statements are presented fairly, in all material respects;
- five internal control deficiencies requiring management's attention; however, we do not consider them to be material weaknesses;
- five instances of noncompliance or other matters required to be reported under Government Auditing Standards; and
- adequate resolution of the prior year's audit findings.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Firewall Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Christopher Newport University (University) does not properly secure its firewall in accordance with its information security standard, the Commonwealth's Information Security Standard, SEC 501 (Security Standard).

We communicated five separate control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires the documentation and implementation of certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data.

The University should develop a plan to implement the controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard in a timely manner. Doing this will help to ensure the University secures the firewall to protect its sensitive and mission critical data.

Improve Policies and Procedures over System Access Removal for Terminated Employees
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not remove terminated employees' system access in a timely manner in accordance with their policies and procedures. University employees retained access to the University's accounting and financial reporting system and the Commonwealth's purchasing and human resource systems after their termination date as follows:

- Four of eighteen employees (22%) with access to the Commonwealth's purchasing system did not have their access removed until between two weeks and four months following their termination.

- The University could not provide sufficient documentation supporting the timely removal of two of ten employees (20%) with access to the University's accounting and financial reporting system.

- The former Director of Human Resources did not have their access to the Commonwealth's personnel management system removed until over a week after their termination.

- One of seventeen (6%) terminated employees maintained active University login credentials for over three months.

The University has elected to model its information security policies and procedures after the Security Standard. The Security Standard, *Section PS-4 Personnel Termination*, requires an organization to disable information system access within 24-hours of termination of employment. The University's current policies and procedures require removal of system access within three days of termination for all information systems with the exception of the Commonwealth's purchasing system which allows seven days for system access to be terminated. Untimely removal of access to information systems can expose the University to inappropriate activity by individuals no longer employed by the institution. Untimely user access deactivations may compromise the protection and integrity of confidential purchasing and accounting and financial reporting system data.

The University did not remove employees' access to systems timely due to miscommunication and lack of oversight by responsible parties. In addition, management attributed some instances of delay in access removal to functionality issues with the University's employee management system, which notifies management of terminations and the need to remove access. In these instances, users did not promptly receive a notification from the system informing responsible parties that access removal was required for a terminating employee.

The University should update its written internal policies and procedures, implementing stricter requirements that ensure employee access to information systems is removed in a timely manner in accordance with policies and procedures. The University should also ensure that these policies and procedures align with requirements outlined in the Security Standard. The University should implement additional requirements for notification by supervisors to expedite the access removal process, as employees often provide two weeks' notice when separating. If the University continues to use its employee management system, management should also ensure that it is working effectively as intended and that system issues are immediately identified and promptly addressed.

Improve Virtual Private Network Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not properly secure its virtual private network in accordance with its information security standard.

We communicated one separate control weakness to management in a separate document marked FOIA Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires the documentation and implementation of certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data.

The University should develop a plan to implement the control discussed in the communication marked FOIA Exempt in accordance with the Security Standard in a timely manner. Doing this will help to ensure the University secures the virtual private network to protect its sensitive and mission critical data.

Implement Formal Policies and Procedures over Conflict of Interest Requirements

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University's procedures over Statements of Economic Interest (SOEI) filings are not adequate to ensure compliance with the Code of Virginia requirements. As an example, their procedures do not require University staff to complete and file financial disclosure forms prior to assuming a position of trust, but allow it to be completed later. Additionally, nine out of thirty-two filers (28%) did not complete the mandatory SOEI training within the required timeframe; for each of these filers, completion of this training was months or years overdue.

The Code of Virginia § 2.2-3114A and § 2.2-3118.2 requires individuals in positions of trust to file a disclosure statement of their personal interests with the Commonwealth Ethics Council on or before the day their position is assumed. Thereafter, these individuals must complete and submit this statement annually on or before February 1. Additionally, the Conflict of Interest Act requires filers to complete orientation training to help them recognize potential conflicts of interest. This orientation must be completed within two months of hire and at least once during each consecutive period of two calendar years.

The University could be susceptible to actual or perceived conflicts of interest that would impair or appear to impair the objectivity of certain programmatic or fiscal decisions made by employees in designated positions of trust. By not ensuring that all required employees have completed the necessary disclosures and training, the University may be prevented from relying on its employees to effectively recognize, disclose, and resolve conflicts of interest. While not a cost to the University, employees in a position of trust who do not complete the required SOEI form may, as allowed by the Code of Virginia § 2.2-3124, be assessed a civil penalty in an amount equal to $250.

Human Resources management was not aware of the Code of Virginia requirement directing all individuals in a position of trust to complete an SOEI form prior to assuming their position. Additionally, University management does not have sufficient written policies and procedures in place to adequately monitor filers to ensure that they meet SOEI training requirements.

Human Resources management should implement formal policies and procedures to ensure all requirements for the SOEI are met. These policies should incorporate guidance issued by the Commonwealth's Ethics Council. Additionally, management should monitor all employees designated in a position of trust to ensure they complete the required SOEI training once within each consecutive period of two calendar years and maintain a record of such attendance.

Improve Web Application Security

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not properly secure a sensitive web application in accordance with its information security standard.

We communicated one control weakness to management in a separate document marked FOIA Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires the documentation and implementation of certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data.

The University should develop a plan to implement the control discussed in the communication marked FOIA Exempt in accordance with the Security Standard in a timely manner. Doing this will help to ensure the University secures the web application to protect its sensitive and mission critical data.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

May 15, 2020

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
Christopher Newport University

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of Christopher Newport University as of and for the year ended June 30, 2019, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated May 15, 2020. Our report includes a reference to other auditors. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of the University, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

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 to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

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 over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. We did identify certain deficiencies in internal control over financial reporting entitled "Improve Firewall Security," "Improve Policies and Procedures over System Access Removal for Terminated Employees," "Improve Virtual Private Network Security," "Implement Formal Policies and Procedures over Conflict of Interest Requirements," and "Improve Web Application Security," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

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 instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings entitled "Improve Firewall Security," "Improve Policies and Procedures over System Access Removal for Terminated Employees," "Improve Virtual Private Network Security," "Implement Formal Policies and Procedures over Conflict of Interest Requirements," and "Improve Web Application Security."

The University's Response to Findings

We discussed this report with management at an exit conference held on May 20, 2020. The University's response to the findings identified in our audit is described in the accompanying section titled "Agency Response." The University's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings

The University has taken adequate corrective action with respect to audit findings reported in the prior year.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

LCW/vks

CHRISTOPHER NEWPORT
UNIVERSITY

May 15, 2020

Martha S. Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Mavredes:

Christopher Newport University has reviewed the findings and recommendations provided by the Auditor of Public Accounts for fiscal year ended June 30, 2019. The University appreciates the effort and hard work the APA auditors put towards the audit this year and has the following response to the Internal Control and Compliance Matters:

Internal Control and Compliance Matters

Improve Firewall Security

The University will implement controls to ensure the University secures the firewall to protect its sensitive and mission critical data.

Improve Policies and Procedures over System Access Removal for Terminated Employees

Policies and procedures will be updated and controls implemented to ensure employee access to information systems is removed in a timely matter and in accordance with policies and procedures.

Improve Virtual Private Network Security

The University is in the process of implementing a multi-factor authentication for remote access.

Implement Formal Policies and Procedures over Conflict of Interest Requirements

Policies and procedures will be updated to ensure control and compliance over the Statement of Economic Interest requirements are met. Currently, all filers have completed the required form and employees have completed the required training.

Office of the Executive Vice President, 1 Avenue of the Arts, Newport News, VA 23606
Phone: 757-594-7040 Fax: 757-594-7864

Improve Web Application Security

Policies, procedures and documentation will be implemented to ensure security over web-accessible applications are in accordance with Systems and Software Security Patching Standards.

Sincerely,

William L. Brauer
Executive Vice President

Office of the Executive Vice President, 1 Avenue of the Arts, Newport News, VA 23606
Phone: 757-594-7040 Fax: 757-594-7864

CHRISTOPHER NEWPORT UNIVERSITY

As of June 30, 2019

BOARD OF VISITORS

Robert R. Hatten, Rector
C. Bradford Hunter, Vice Rector
Terri M. McKnight, Secretary

William R. Ermatinger
Maria Herbert
W. Bruce Jennings
Steven S. Kast
Gabriel A. Morgan, Sr.
Lindsey C. Smith
Kellye L. Walker
Ella P. Ward
Judy F. Wason
Junius H. Williams, Jr.

Tatiana Rizova, Faculty Representative
Henry Womble, Student Representative

UNIVERSITY OFFICIALS

Paul S. Trible, President

David C. Doughty, Provost

Cynthia R. Perry, Chief of Staff

William L. Brauer, Executive Vice President

Kevin Hughes, Vice President of Student Affairs

Jennifer Latour, Vice President for Strategy and Planning

Lisa Duncan-Raines, Vice President for Enrollment and Student Success

Adelia P. Thompson, Vice President of University Advancement