CHRISTOPHER NEWPORT UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2017

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, 2017, and issued our report thereon, dated May 4, 2018. Our report is included in the University's Financial Statements that it anticipates releasing on or around June 8, 2018. Our audit found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses;
- 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

Perform Periodic Vulnerability Scans

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

Christopher Newport University (University) did not perform periodic vulnerability scans to evaluate potential vulnerabilities on a mission critical system. The University performed a vulnerability scan in June 2017 for a mission critical system, but did not perform any subsequent scans until January 2018.

We communicated the details about the existing vulnerabilities to management in a separate document marked Freedom of Information Act Exempt under §2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls.

The University's *Security Control Periodic Review Procedure* requires the University to scan for vulnerabilities within every 30 days, or more frequent depending on criticality of newly industry-discovered vulnerabilities. In addition, the University's adopted information security standard, the Commonwealth's Information Security Standard, SEC 501, requires the University to scan for vulnerabilities in sensitive information systems at least every 90 days and when new vulnerabilities potentially affecting the system are identified and reported.

Conducting vulnerability scans on mission critical and sensitive systems allows system administrators to determine if newly discovered vulnerabilities exist in the system. By not performing periodic vulnerability scans, the University is unable to evaluate and remediate potential vulnerabilities that malicious users could discover and exploit to compromise mission critical systems and sensitive data. The University acknowledged the Information Security Officer failed to include the new system in the periodic scans according to policy.

The University should perform periodic vulnerability scans and evaluate the results to determine if newly discovered vulnerabilities exist. The University should also dedicate the necessary resources to remediate vulnerabilities on a timely basis. Doing this will help to ensure the confidentiality, integrity, and availability of the University's sensitive and mission critical data.

Improve Controls over Purchasing System Access

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

The University is not removing access for terminated employees from the Commonwealth's purchasing system (system) in a timely manner. The University's Security Officers did not remove system access timely for two of 14 (14 percent) terminated employees with purchasing system access. This

access was removed 88 and 264 days late, respectively. In addition, the University is not limiting system access of certain roles to only those users requiring access to perform job duties. Ten out of 226 employees (four percent) had unnecessary access to the purchasing system roles given their job duties.

The University's Security Plan requires Security Officers to deactivate terminated user accounts within the period established by the Office of Human Resources' Employee Separation Clearance Policy. This policy requires deactivation within three business days of employee separation. Furthermore, the Commonwealth's purchasing system security standards also require terminations be reported immediately to the applicable security officer so action can be taken to deactivate access as needed. Lastly, best practices dictate that entities should assign system access based on the concept of least privilege.

Inappropriate or unnecessary access to the University's purchasing system reduces management's ability, in the normal course of performing their assigned functions, to prevent, or detect errors on a timely basis. In addition, there is an increased risk of fraudulent purchases by terminated employees with purchasing system access. Timely submission of the request to delete access for terminated employees is imperative to safeguard the assets of the Commonwealth.

The untimely deactivation of system access for terminated employees is due to miscommunication and a lack of oversight between the supervisors and the Security Officers. The unnecessary system access was due to the University's policy to assign certain roles to all users regardless of need.

The University should ensure timely deactivation of terminated employee access to the system by ensuring coordination between those designated to submit the request for deactivation and the Security Officers responsible for removal. The University should also update their policy regarding which roles they assign to all users to ensure system access is granted in accordance with the least privilege concept.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

May 4, 2018

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** (the University) as of and for the year ended June 30, 2017, 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 4, 2018. 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 "Perform Periodic Vulnerability Scans" and "Improve Controls over Purchasing System Access," 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 "Perform Periodic Vulnerability Scans" and "Improve Controls over Purchasing System Access."

The University's Response to Findings

We discussed this report with management at an exit conference held on May 15, 2018. The University's response to the findings identified in our audit is described in the accompanying section titled "University 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 Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

AUDITOR OF PUBLIC ACCOUNTS

LCW/alh

CHRISTOPHER NEWPORT
UNIVERSITY

May 4, 2018

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, 2017. 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 Matter:

Internal Control and Compliance Matters

Perform Periodic Vulnerability Scans

The University will ensure that the necessary resources are dedicated to implement the controls, as discussed in the communication marked FOIA Exempt in accordance with the Security Standard, in a timely manner.

Improve Controls over Purchasing System Access

The University will ensure timely deactivation of terminated employee access to the system and apply the concept of least privilege when granting system access.

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, 2017

BOARD OF VISITORS

N. Scott Millar
Rector

Vicki Siokis Freeman
Vice Rector

C. Bradford Hunter
Secretary

Lindsey A. Carney
William R. Ermatinger
Robert R. Hatten
Mr. S. Anderson Hughes
W. Bruce Jennings
Steven S. Kast
Terri M. McKnight
Gabriel A. Morgan, Sr.
Kellye L. Walker
Ella P. Ward
Preston M. White, Jr.

Brian Puaca
Faculty Representative

Kenneth Kidd
Student Representative

UNIVERSITY OFFICIALS

Paul S. Trible, President

David C. Doughty, Provost

Cynthia R. Perry, Chief of Staff

William L. Brauer, Executive Vice President

Adelia S. Thompson, Vice President of University Advancement