LONGWOOD UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2016

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 Longwood University as of and for the year ended June 30, 2016, and issued our report thereon, dated September 20, 2017. Our report is included in the University's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.longwood.edu. 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; and
- instances of noncompliance with applicable laws and regulations or other matters that are required to be reported under Government Auditing Standards.

–TABLE OF CONTENTS–

STATUS OF PRIOR YEAR FINDINGS

Improve Virtual Private Network Security

Longwood University (University) is making progress to address a weakness communicated in our prior year report in virtual private network (VPN) controls; however, the corrective action remains in progress. Specifically, the University identified additional security equipment that, when implemented, should reduce this risk to a reasonable level and better align VPN controls with industry best practices. Additionally, the University made progress in implementing controls to improve VPN software patching and user training; however, the corrective actions are not complete. The University's adopted information security standard, ISO 27002, and industry best practices, such as the Special Publication 800-53r4 published by the National Institute for Standards and Technology, require and recommend specific VPN configuration settings to better ensure the adequate protection of remotely accessed information technology resources.

The University plans to finish the equipment implementation and corrective action by December 31, 2017. The fiscal year 2017 audit will include an evaluation of the University's completed corrective action and determine whether the University satisfactorily resolved the weakness.

Improve Oversight of Third-Party Service Providers

The University is making progress to address a weakness communicated in our prior year report related to maintaining oversight of third-party service providers; however, the corrective action remains ongoing. Specifically, the University developed a Data Protection Addendum that defines data protection requirements and methods for obtaining assurance. However, the University is still working to develop a formal process to identify contracts that require including the Data Protection Addendum. Additionally, the University does not have a formal review process for obtaining assurance and approving the technical stipulations of a contract by an authorized and qualified individual, which should be included in the corrective action plan. The University must establish requirements in its contractual agreements with service providers to protect sensitive data up to or exceeding the requirements of the University's adopted information security standard, ISO 27002 and University policies.

The University should verify the corrective action addresses all weaknesses communicated in the recommendation, which the University plans to finish by December 31, 2017. The fiscal year 2017 audit will include an evaluation of the University's completed corrective action and determine whether the University satisfactorily resolved the weakness.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Annual Financial Statement Reporting Procedures

University management should improve procedures for compiling the annual financial statements. During the audit, the following deficiencies were noted:

- Construction in Progress was overstated and depreciable assets was understated by a net $12.6 million dollars. This was attributable to expenses for two capital projects totaling $14.7 million not being reclassified from non-depreciable to depreciable assets, even though they were deemed substantially complete. The total overstatement was offset by an oversight of $2.1 million of capital related expenses not being recorded in Construction in Progress;
- A total of $3.3 million and $1.1 million was not properly recognized within the appropriate auxiliary and operation and maintenance expense categories, respectively;
- The University experienced delays in obtaining supporting documentation to provide a solid audit trail for Foundation reporting; and
- Existing procedures for performing inventory, completing surplus forms, and reporting fixed assets in the annual financial statements need to be strengthened.

Financial Reporting, Campus Planning and Construction and Foundation management should collaborate to enhance procedures for compiling the annual financial statements. The procedures should ensure all University activity is properly accounted for and reported in the financial statements and include a review process to ensure errors are identified and corrected.

Develop Procedures for Tracking Time and Effort on Federal Awards

The Office of Sponsored Programs does not have an established process for tracking time and effort on Federal awards. The Federal Uniform Guidance requires that institutions have a method for ensuring that charges to Federal awards for salaries and wages are based upon institutional records that accurately reflect the work performed. The Office of Sponsored Programs should develop comprehensive policies and procedures that align with Federal regulations for tracking time and effort on Federal awards and ensure those University policies are disseminated to employees with Federal research responsibilities. The Office of Sponsored Programs should also implement a formal process for tracking time and effort to prevent charges to federal awards from being deemed unallowable.

Improve Information Security Officer Independence and Risk Acceptance Process

The University does not position its Information Security Officer (ISO) role in an area or department that is independent from the Director of Information Technology (IT Director). Additionally, the University does not regularly include business process owners in the IT risk acceptance process. The University's organizational structure includes a dotted line from the ISO to the Chief Information Officer (CIO); however, this control does not alleviate the independence concerns associated with the placement of the

ISO since the CIO, like the IT Director, faces competing priorities that may limit the effectiveness of the ISO role. The University's adopted information security standard, ISO 27002 (Security Standard) states that conflicting duties and areas of responsibility, such as IT operations and IT security, should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets (*Security Standard section: 6.1.2 Segregation of duties*).

Appropriate segregation of duties should be established within the organizational structure to enable adequate execution of both operational and security functions. The ISO should report directly to the President, if practical, or to another senior leadership position outside of the IT department. Having the ISO role report to the IT Director or CIO may limit effective assessment and the subsequent recommendation of security controls, and assignment of security control responsibilities across the University's IT environment due to possible competing priorities that sometimes face the IT operations leadership. Additionally, the ISO does not currently have the capability to objectively report on the status of IT security to the University's executive business leadership.

The ISO facilitates the completion of IT risk assessments and, when vulnerabilities are identified during the risk assessment process, the system owner must provide a mitigation plan or document acceptance of the risk for each vulnerability. However, when a system owner chooses to accept a risk, the University does not have a process to communicate that risk to other business process owners who are impacted by that system to ensure they are in agreement with the risk acceptance. Without a sufficient risk acceptance process, business process owners may not be aware of the risks which can impact the availability of the systems that support their business processes.

The lack of an ISO positioned outside of the operational department for which the ISO writes and reviews security controls could weaken the overall security posture of the University. Additionally, without an objective reporting structure for the ISO, the University's leadership may not be aware of the security risks the University faces and will not allocate the necessary resources to reduce risk and ensure the confidentiality, integrity, and availability of sensitive data stored or processed by University systems.

These controls are not implemented because the University has not considered the risks associated with the current governance structure, even after adding the dotted line from the ISO to CIO, and risk assessment reporting process. The ISO's lack of effectiveness in the current organizational structure may also be a contributing factor to the other IT recommendations issued during the previous and current year audits.

The University should evaluate the organizational placement of the ISO to eliminate any conflicts of interest in the implementation of the Information Security Program and controls. While it may not be feasible for the ISO to report directly to the President, the University should consider placing the ISO role in a different organizational unit that reports to a different executive level position. Additionally, the University should develop a process to allow the ISO to objectively report on the status of information security and risk assessments, as needed, to the President and executive leadership. Also, the University should implement a process to include business process owners in the IT risk acceptance process. Making these improvements to the University's IT governance will increase the ability to identify, report, and mitigate risks and continue to mature its information security program.

Improve Continuity of Operations Planning

The University does not have a Continuity of Operations Plan (COOP) that reflects the current information technology (IT) environment. Additionally, the University does not verify that the COOP has appropriate restoration requirements, is consistent with the Disaster Recovery Plan (DRP), and is in compliance with the University's information security standard, ISO 27002 (Security Standard).

The University's department of Emergency Management is collecting departmental information about what IT systems are required to support business functions; however, this information and documentation is not complete. Additionally, the Emergency Management and Information Technology Services departments have not collaborated to verify the accuracy of the IT system information provided and prioritized it accordingly. Collaboration is required to verify that the system and restoration requirements documented in the business impact analysis section of the COOP are consistent with the technical information and restoration plans in the DRP.

The Security Standard defines minimum requirements for continuity planning to ensure that systems are restored in a timely manner to support primary business functions (*Security Standard section: 17 Information security aspects of business continuity management*). The lack of a complete and accurate COOP that is consistent with the DRP increases the risk that the University cannot prioritize system restoration to support mission essential business functions. Additionally, with an incomplete COOP, the University cannot thoroughly test the COOP and the DRP to ensure that Information Technology Services has the capability to restore critical systems within the defined recovery time objectives.

The University should complete the COOP and verify that it reflects current business functions and supporting IT systems. Additionally, the University should dedicate resources to establish a collaborative relationship between Emergency Management and Information Technology Services to ensure consistency between the information and restoration requirements documented in the COOP and DRP.

Improve System Hardening for Server Operating Systems

The University is missing some critical security controls for the server operating system where the primary financial management system's database resides. These missing controls are either required by the University's information security standard, ISO 27002, or recommended by industry best practices, such as the Center for Internet Security.

We communicated the details of the control weaknesses to the University in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security mechanisms. Generally, the weaknesses were related to system hardening and least functionality.

The University should dedicate the necessary resources to implement the controls communicated in the FOIAE document. Doing this will improve the information security and reduce the risks to the University's sensitive and financial data.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 20, 2017

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
Longwood 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 **Longwood University** (University) as of and for the year ended June 30, 2016, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated September 20, 2017. 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 Annual Financial Statement Reporting Procedures," "Develop Procedures for Tracking Time and Effort on Federal Awards," Improve Information Technology Officer Independence and Risk Acceptance Process," Improve Continuity of Operations Planning" and "Improve System Hardening for Server Operating Systems" 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 an instance of noncompliance entitled "Develop Procedures for Tracking Time and Effort on Federal Awards" required to be reported under Government Auditing Standards and which is described in the section titled "Internal Control and Compliance Findings and Recommendations."

The University's Response to Findings

We discussed this report with management at an exit conference held on August 4, 2017. 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

With respect to all audit findings reported in the prior year, the University has completed some corrective actions, while others remain ongoing. Accordingly, we included the status of findings entitled

"Improve Virtual Private Network Security" and "Improve Oversight of Third-Party Service Providers" in the section entitled "Status of Prior Year Findings."

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

JRQ/alh

LONGWOOD
UNIVERSITY

201 High Street
Farmville, Virginia 23909
tel: 434.395.2016
fax: 434.395.2635
trs: 711

Office of the Vice President for Administration and Finance

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

Dear Ms. Mavredes,

Longwood University has reviewed the Internal Control Findings and Recommendations provided by the Auditor of Public Accounts for fiscal year ending June 30, 2016 and is in agreement, in principle, with all of the findings submitted.

Attached for your consideration is a brief update as to where the campus is with respect to progress on the findings. The formal Corrective Action Workplan will be submitted within thirty days as required by CAPP Manual Section 10205. Please contact me should you have any questions or require additional information.

On behalf of Longwood University, please extend my appreciation to all of your staff for their professional audit work and recommendations.

Sincerely,

Mr. P. Kenneth Copeland, Jr.
Vice President for Administration and Finance

FY 2016 – Internal Control Findings and Recommendations

Improve Virtual Private Network Security

- The ITS department has reviewed the findings, concurs and is implementing corrective actions which will be completed by December 2017.

Improve Oversight of Third-Party Service Providers

- The ITS department and Materiel Management have reviewed the findings, concurs and is implementing corrective actions which will be completed by September 30, 2017.

Improve Annual Financial Statement Reporting Procedures .

- Longwood acknowledges that errors were made when preparing the FY 16 financial statements. To address this issue, the Financial Reporting Analyst has created a "FY 2017 Financial Statement Preparation Plan" which includes time for the adequate review of entries and submissions before the applicable due date by the Associate VP for Administration and Finance and by the VP for Administration and Finance when deemed appropriate. The final statements will be reviewed by the Associate VP for Administration and Finance and the VP for Administration and Finance.

  The FY 2017 Financial Statement Preparation Plan incorporates the Fixed Asset Accountant, Capital Design & Construction Financial and Budget Specialist, Foundations, Budget Office, General Accounting, and other departments across campus that provide information (such as inventory) to ensure that the information provided in the statements is timely, accurate and complete.

  On-Line training provided by the Department of Accounts, Department of Accounts Financial Reporting staff and contacts at other higher education institutions will be utilized to ensure the accurate treatment of items when in doubt. Longwood is committed to ensure that the FY 17 financial statements and subsequent statements are accurate, complete and submitted timely.

Develop Procedures for Tracking Time and Effort on Federal Awards

- Effective April 25, 2017, the Grants – Post Award duties were moved to Financial Operations and now report to the Associate VP for Administration and Finance. The position is currently housed in the Office of Sponsored Programs to provide a seamless transition between pre-award and post-award functions for the Principal Investigator (PI).

  The Grants – Post Award Office is currently reviewing OMB guidance and reaching out to other universities to develop an effective process for tracking time and effort on federal grants. These policies and procedures will be clearly documented and included on the Office of Sponsored Programs website by September 30, 2017.

Improve Information Security Officer Independence and Risk Acceptance Process

- The ITS department has reviewed the findings, concurs and is implementing corrective actions which will be completed by June 06, 2017.

Improve Continuity of Operations Planning

- The ITS department has reviewed the findings, concurs and is working with the Emergency Management department to implement corrective actions which will be completed by April 2018.

Improve System Hardening for Server Operating Systems

- The ITS department has reviewed the findings, concurs and is implementing corrective actions which will be completed by Implementing CIS Foundational Benchmarks December 2017.

LONGWOOD UNIVERSITY

Farmville, Virginia
As of June 30, 2016

BOARD OF VISITORS

Robert S. Wertz, Jr.
Rector

Marianne M. Radcliff
Vice Rector

Eileen M. Anderson
Katharine M. Bond
Katherine E. Busser
Michael A. Evans
Steven P. Gould
David H. Hallock, Jr.
Eric Hansen
Colleen M. Margiloff
Stephen L. Mobley
Nettie L. Simon-Owens
Lucia Anna Trigiani

UNIVERSITY OFFICIALS

W. Taylor Reveley, IV
President

Joan Neff
Provost and Vice President for Academic Affairs

Ken Copeland
Vice President for Administration and Finance

Tim Pierson
Vice President for Student Affairs

Victoria Kindon
Vice President for Strategic Operations

Courtney Hodges
Vice President for University Advancement