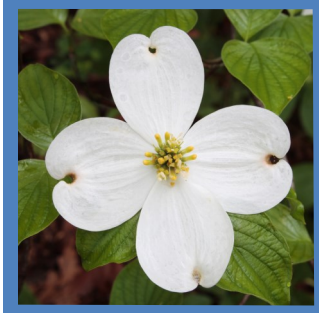


VIRGINIA STATE UNIVERSITY

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 Virginia State University as of and for the year ended June 30, 2016, and issued our report thereon, dated June 22, 2017. Our report, including in the University's Financial Statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.vsu.edu.

Our audit of Virginia State University for the year ended June 30, 2016, 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 or other matters required to be reported under Government Auditing Standards.

Our audit also included testing over federal Student Financial Assistance in accordance with the U.S. Office of Management and Budget Compliance Supplement Part 5 Student Financial Assistance Programs; and found no internal control findings requiring management's attention or instances of noncompliance in relation to this testing.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve the Change and Configuration Management Process

The University should continue to formalize its current change and configuration management policy and procedures for its primary system-of-record for student and financial data. The Commonwealth's Information Security Standard, SEC 501-09 (Security Standard), Section CM-1, requires the University to develop, document, implement, and review annually thereafter, a configuration management policy and procedure.

Without a complete, organized and comprehensive policy and procedure, the University introduces a risk that changes are implemented without appropriate approval and testing. Unauthorized changes present a risk for outages across the University's information technology (IT) environment that would hinder the University from performing its mission-essential functions.

The delay in establishing a formal change and configuration management process is due to the University's IT project prioritizations. In conjunction with nine full-time IT vacancies and limited financial resources, other higher prioritized projects have taken precedence. The University should allocate the necessary resources to formalize its change and configuration management process for its primary system-of-record for financial and student data.

Improve User Access Controls

Our review of user access over various systems identified the following:

- Technology Services does not consistently remove terminated employees' access to administrative systems on their last day of work. For four of 49 instances where terminated employees had access to administrative systems, several months had passed since the employees terminated, but their access to administrative systems remained active. Further, Technology Services provided no evidence that it conducted an annual review of users with access to its administrative system.

- The University's procurement security officer did not remove terminated employees' access to the procurement system timely. For three out of 12 instances where terminated employees had procurement system access, several months had passed since the employees terminated, but their access remained active.

- The Residence Life and Housing Department (Housing) is not reviewing user accounts for reasonableness, deactivating inactive accounts, or limiting system administrator rights to individuals responsible for maintaining a departmental system. Further, Housing does not annually review user access to ensure that job duties have not changed that would necessitate a change in access privileges.

Despite any mitigating controls, such as automatic password expiration and removal of access in Active Directory, security officers must remove access to all applications used by terminating employees. Part D of the University's Policy 6310 *Logical Access Control and Account Management Policy,* requires the immediate termination of user access to all systems effective on the employees last day of work. This policy is consistent with and was developed to promote the University's compliance with the Security Standard, Section PS-4, *Personnel Termination*. Further, University Policy 6310.C.6 requires that University departments annually review user accounts and sign off that the access is reasonable and this policy is consistent with the Security Standard, Section AC-2j. Reviewing accounts at least annually serves to minimize the risks associated with user accounts that were not properly deleted during the year or users with access to modify or view information not necessary to perform their jobs. The University's departments should comply with University Policy 6310 by immediately deleting terminated employee access to all systems, assigning access based on the principle of least privilege, and performing an annual review of access to ensure the granted roles are appropriate based on the employee's job duties.

Enforce Contract Administration and Vendor Payment Controls

The University did not follow internal controls over contract administration and invoice processing for one vendor, resulting in an overpayment totaling $20,275. Specifically, in December 2015, Student Activities paid an invoice; however, no payment was due and instead, the vendor owed the University money from ticket sale revenue collected by the vendor but not turned over to the University. The Contract Administrator approved the invoice for payment even though the invoice did not adhere to the contract terms and the vendor provided no support for amounts used in his calculations.

The contract related to this vendor includes addendums with varying profit sharing percentages and arrangements. For example, the contract requires the vendor to pay all costs upfront; however, the University provided a cash pre-payment to the vendor a day before the event occurred, which he used to cover the costs. In addition, the contract states that the vendor should assist the University in securing contracts with performing artists; however, the vendor negotiated his own contracts with those artists and the contracts did not include all the terms and conditions typically required by the University and Commonwealth of Virginia.

The University should require that the vendor reimburse the University for the $20,275 overpaid. The vendor invoiced the University for amounts inconsistent with the contract terms and provided no support for a majority of claimed expenses. Further, the University should review the existing contract and consider contract modifications to ensure the contract clearly articulates what constitutes adequate support for claimed expenses, and how the vendor should calculate net profit and amounts due.

Update Contract Provisions, Enforce Contract Administration, and Evaluate Supporting Documentation and Reasonableness of Federal Grant Expenditures

The University entered into a contract with Personal Communications Industry Association (PCIA) for the Catalog of Federal Domestic Assistance (CFDA) #17.282 "Trade Adjustment Assistance Community College and Career Training (TAACCCT)." We reviewed thirteen vouchers associated with

this grant and found that two vouchers from PCIA did not have adequate supporting documentation and did not comply with contract requirements, resulting in known questioned costs of $241,203.

Financial management requirements outlined in the U.S. Office of Management and Budget (OMB), Uniform Guidance, Section 200.302, requires that each state must expend and account for the Federal award in accordance with state laws and procedures for expending and accounting for the state's own funds. University procedures require contract administrators to provide assurance that the vendor adheres to contract specifications, terms, and conditions; and the University's contract with PCIA requires monthly invoices that must include a description, price, and quantity for all costs incurred. For the two PCIA vouchers reviewed:

- One voucher for $7,177 included a coversheet with a statement that the requested expenditure reimbursement relates to TAACCCT, the requested reimbursement amount, and a signature from the Chief Executive Officer of PCIA, but it did not include the required description, price, and quantity.

- One voucher for $234,026, representing 39.6 percent of the University's total fiscal year 2016 expenditures for TAACCCT, included an outline of the contract's deliverables; however, there was no documentation specifying the cost for these deliverables or evidence that PCIA provided the deliverables. Additionally, this voucher covered one year of work, whereas the contract specifies that PCIA must submit invoices monthly. Lastly, there is no evidence that a contract administrator or program manager reviewed the voucher to determine that the University received the stated deliverables and that the amount requested was reasonable.

Since the University pays the PCIA invoices with federal funds, failure to obtain adequate supporting documentation for the grant expenditures could result in the U.S. Department of Labor requiring repayment of the federal funds, revoking current funding for the grant and jeopardizing future federal funding.

The University should require all vendors to provide invoices in compliance with the contract terms and supporting documentation, including details such as description of services, price and quantity.

Match Federal Grants with Qualifying State Expenses

In April 2016, the U.S. Department of Agriculture (Agriculture) conducted a performance and administrative review of the University's National Institute of Food and Agriculture (NIFA) sponsored programs for fiscal year 2014. The review disallowed 2014 indirect cost recoveries that the University claimed as state matching funds, but in September 2016 Agriculture accepted the University's plan to replace some of the 2014 indirect costs with qualifying educational expenses related to teaching. Subsequently, Agriculture sent a memo to all 1890 Land-grant University Presidents clarifying that it is unallowable to apply qualifying educational expenses to state match unless NIFA provides prior approval.

The Code of Federal Regulations, 7 C.F.R. §3419.6, requires matching funds to be used for agricultural research and extension activities that have been approved in the plan of work required under sections 1444(d) and 1445(c) of the National Agricultural Research, Extension, and Teaching Policy Act of 1977 (NARETPA). NARETPA sections 1444 and 1445 state that indirect costs are unallowable as program grant expenditures.

Being unaware at the time that it could not claim indirect cost recoveries as state matching funds, the University charged $1,439,298 and $1,070,700 as such during fiscal years 2015 and 2016, respectively. They discontinued doing so in May 2016, upon receiving the results of Agriculture's review. Agriculture's approval for the University to replace 2014 indirect costs recoveries with qualifying educational expenses only applied to the 2014 fiscal year and as of current, the University has not held negotiations with NIFA regarding the state fund match for fiscal years 2015 and 2016, resulting in questioned costs totaling $2,509,998.

The University should request Agriculture's approval to replace the 2015 and 2016 unallowable indirect cost recoveries with qualifying educational expenses related to teaching and provide all documentation to support those expenses. In addition, the University should not charge future indirect cost recoveries to NIFA programs and avoid charging qualifying educational expenses without Agriculture's prior approval.

Continue Improving Oversight over Third-Party Service Providers

The University continues to develop a formal process to improve oversight over its third-party service providers (providers) that run certain IT functions on behalf of the University. These IT functions include the University's financial and student systems.

During the prior year audit, we identified eight weaknesses related to provider oversight. The University has resolved one weakness and is continuing to implement corrective actions and resolve the remaining seven. The University is working on a process to gain a better understanding of their providers' IT environment and security controls. Additionally, the University has an engagement with an external consultant to provide guidance for developing a process to consistently evaluate independent audit assurance from providers.

Section SA-1 of the Commonwealth's Hosted Environment Information Security Standard, SEC-525 (Hosted Environment Standard), requires the University to develop, document, and implement appropriate system and services acquisition policies and procedures. Also, Section SA-9-COV-3 requires the University perform an annual security audit or review the annual audit report of the provider's environment conducted by an independent third-party audit firm.

Until the University completes its formal documented process for overseeing its providers, the University is at risk of not complying with the Hosted Environment Standard, and the University further risks not obtaining assurance that the provider's internal control environment is sufficient to protect Commonwealth data.

The delay in correcting these deficiencies during the past year is due to the University's IT project prioritizations. In conjunction with nine full-time IT vacancies and limited financial resources, other higher prioritized projects took precedence last year. The University now estimates to have a process to review third-party providers by the end of calendar year 2017.

The University should continue implementing its corrective actions to resolve the remaining weaknesses identified in the prior audit and develop a formal process to maintain oversight over its providers. By developing a formal process, the University will gain assurance that the providers' IT controls are operating effectively to protect the confidentiality, integrity, and availability of sensitive and mission-critical systems.

Continue Improving Risk Management and IT Security Audit Plan Documents

The University risk management documentation continues to be inconsistent. As a result, the University produced inaccurate and incomplete contingency planning documents and an IT Security Audit Plan that omits some sensitive IT systems from scheduled reviews. Risk management documents include the University's Business Impact Analysis (BIA), IT System and Data Sensitivity Classifications (Sensitivity Classifications), and IT System Risk Assessments (RA). Contingency planning documents include the University's Continuity of Operations and Disaster Recovery Plans.

The University does not fulfill IT risk management and contingency planning requirements as set forth in the Security Standard, Sections three through six and CP-1 through CP-2. The University's incomplete and inconsistent risk management documentation is also resulting in deviations from the Commonwealth's IT Security Audit Standard, SEC-502 (IT Audit Standard), Sections 1.4 and 2.1.

These inconsistencies increase the risk that IT systems do not have the appropriate information security controls to protect sensitive information. Additionally, an inaccurate IT Security Audit Plan increases the risk that vulnerabilities and threats go undetected and not remediated. Lastly, the University's outdated and inconsistent contingency plans may prevent the University from restoring certain mission-essential business functions in a timely manner in the event of a disaster or outage.

The delay in addressing its risk management and IT Security Audit Plan documents is due to the University's IT project prioritizations. In conjunction with nine full-time IT vacancies and limited financial resources, other higher prioritized projects has taken precedence.

The University should evaluate and update the risk management documents to consistently identify and prioritize essential business functions and supporting IT systems to reflect the University's current environment. In addition, the University should consistently classify the sensitivity of IT systems to ensure appropriate implementation of information security controls to mitigate system vulnerabilities and threats. Lastly, the University should use the risk management documentation as the primary input for the contingency planning documents and IT Security Audit Plan to ensure the documents are consistent and comply with the Security Standard and IT Audit Standard.

Continue Addressing Weaknesses from Information Security Audits

The University continues to address the information security weaknesses found during fiscal year 2015 security audits of two sensitive systems that require certain security controls to protect data. The information security audits reviewed compliance with the Security Standard and found that each system does not comply with 92 percent of applicable information system security controls as required by the Security Standard.

The University has replaced one system and is currently replacing the other system with an expected completion date of December of 2017 to resolve the security control weaknesses and comply with the Security Standard and industry best practices. The University should continue to dedicate the necessary resources to ensure timely completion of its corrective actions and becoming compliant with the Security Standard for systems that process and store sensitive information, such as confidential and mission essential data.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

June 22, 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
Virginia State 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 Virginia State 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 June 22, 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 the Change and Configuration Management Process," "Improve User Access Controls," "Enforce Contract Administration and Vendor Payment Controls," "Update Contract Provisions, Enforce Contract Administration, and Evaluate Supporting Documentation and Reasonableness of Federal Grant Expenditures," "Match Federal Grants with Qualifying State Expenses," "Continue Improving Oversight over Third-Party Service Providers," "Continue Improving Risk Management and IT Security Audit Plan Documents," and "Continue Addressing Weaknesses from Information Security Audits," 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 the Change and Configuration Management Process," "Improve User Access Controls," "Update Contract Provisions, Enforce Contract Administration, and Evaluate Supporting Documentation and Reasonableness of Federal Grant Expenditures," "Match Federal Grants with Qualifying State Expenses," "Continue Improving Oversight over Third-Party Service Providers," "Continue Improving Risk Management and IT Security Audit Plan Documents," and "Continue Addressing Weaknesses from Information Security Audits."

The University's Response to Findings

We discussed this report with management at an exit conference held on June 23, 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

The University has partially corrected the previously reported findings titled "Continue Improving Oversight over Third-Party Service Providers," "Continue Improving Risk Management and IT Security Audit Plan Documents," and "Continue Addressing Weaknesses from Information Security Audits." Accordingly, we included these findings in the section entitled "Internal Control and Compliance Findings and Recommendations." The University has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

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

KKH/clj

VIRGINIA STATE UNIVERSITY
P.O. Box 9213
PETERSBURG, VIRGINIA 23806
(804) 524-5995
(804) 524-5347 FAX

Kevin W. Davenport
Vice President for Finance
and Chief Financial Officer

TDD (804) 524-5487

July 21, 2017

Ms. Martha Mavredes
Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218-11295

Dear Ms. Mavredes:

Virginia State University (VSU) has reviewed the Financial Internal Control and Compliance Findings and Recommendations provided by the Auditor of Public Accounts for the year ended June 30, 2016. The University acknowledges and is in agreement, in principle, with the following findings and recommendations:

Improve the Change and Configuration Management Process

The University will improve the Change and Configuration Management Process by continuing to formalize our current change and configuration management policy and procedures for the University's primary system-of-record for student and financial data. The University will work to enhance our current documentation and develop a schedule and alert system for an annual review. We will ensure that our internal procedures and the overall University policy are kept current and consistent.

Improve User Access Controls

The University will continue its efforts to improve and ensure compliance regarding user access control. Technology Services will work with System Owners to ensure that access is reviewed, at least annually, to ensure that the appropriate personnel has access to systems, that terminated employees can no longer access University systems, and that permissions that are in place are consistent with the roles and responsibilities of the staff members who have been granted those permissions. The University will also work to ensure that when employees are terminated from service their access to University automated systems is terminated immediately.

Enforce Contract Administration and Vendor Payment Controls

The University will make the necessary contract modifications to ensure the contract clearly defines the intent of the arrangements with the vendor. Also, VSU will finalize its investigation related to this issue and address any potential overpayments.

Update Contract Provisions, Enforce Contract Administration and Evaluate Supporting Documentation and Reasonableness of Federal Grant Expenditures

The Office of Sponsored Research and Programs (OSRP) will develop procedures and processes for Principal Investigators (PI) to confirm that goods and services were received and that work performed by contractors has been completed prior to providing approval of payment to Accounts Payable. Also, OSRP will provide training and guidance to PIs to ensure they understand and follow the procedures and processes.

Match Federal Grants with Qualifying State Expenses

On June 6, 2017, VSU received a final report from USDA/NIFA for the site visit performed April 4-6, 2016 and the subsequent survey of financial activity of NIFA sponsored programs. After validating a number of expenditures as direct costs and accepting a portion of funding as stand-in costs for Section 1444 Extension funds, the university was asked to return $1,255,591.86 in disallowed costs to the U.S. Treasury. On June 30, 2017, VSU submitted an official request to USDA/NIFA to repay the amount of $1,255,591.86 in equal installments over a period of 5 years. VSU is currently awaiting an official response to the repayment request. In addition to the cited disallowed costs, NIFA included three corrective actions in the site review. The corrective actions included the following areas: 1) Time and Effort Reporting, 2) Identification of Capacity Grant Funds in the Accounting System and 3) Control Gaps in Expenditure Approval Process. VSU is carefully addressing each corrective action and has made significant changes to current fiscal policies and procedures that will prevent any occurrences cited in the 2014 review.

Continue Improving Oversight over Third-Party Service Providers

Technology Services has developed a comprehensive Third-Party Service Provider checklist to ensure that vendors supplying technology services to the University adhere to Commonwealth of Virginia Security policy. During the coming year we will work to both enforce and continue to improve the oversight policy to ensure that the University's automated systems are secure and that Third-Party Service Providers adhere to the contractual agreement set forth by the University.

Continue Improving Risk Management and IT Security Audit Plan Documents

The University will continue to improve its Risk Management and IT Security Audit Plan documents. Although both the Risk Management and Security Audit plans have been approved by Virginia Information Technology Agency, the department will continue to improve the University's overall improvement Risk Management and Audit Plans.

Continue Addressing Weaknesses from Information Security Audits

The University will continue to dedicate the necessary resources to ensure compliance with the Commonwealth of Virginia Security Standard for systems that process and store sensitive information (i.e. confidential and mission essential data).

Virginia State University is committed to addressing these audit findings and recommendations. On behalf of the administration and staff at Virginia State University, please extend my gratitude to your staff for their commitment and professionalism.

Sincerely,

Kevin Davenport
Vice President for Finance and Chief Financial Officer

cc: Dr. Makola M. Abdullah, President
The Honorable Dr. Dietra Trent, Secretary of Education
Mr. David Von Moll, State Comptroller
Mr. Daniel Timberlake, Director of Planning and Budgeting

VIRGINIA STATE UNIVERSITY

As of June 30, 2016

BOARD OF VISITORS

Harry Black, Rector

Willie C. Randall, Vice Rector

Daphne M. Reid, Secretary

Thursa Crittenden
Daryl C. Dance
Robert E. Denton, Jr.
Michael Flemming
Charlie Hill
Alma Hobbs
Frederick S. Humphries, Jr.
Jennifer Hunter
Xavier Richardson
Glenn Sessoms
Wayne Turnage
Huron F. Winstead

Dr. Milton O. Faison, Faculty Representative
Mr. Marshawn Shelton, Student Representative

ADMINISTRATIVE OFFICIALS

As of June 30, 2016

Dr. Makola M. Abdullah
President

Dr. W. Weldon Hill
Vice President for Academic Affairs

Kevin Davenport
Vice President of Administration and Finance

Hubert D. Harris
Chief of Staff

Dr. Letizia Gambrell-Boone
Vice President for Student Affairs