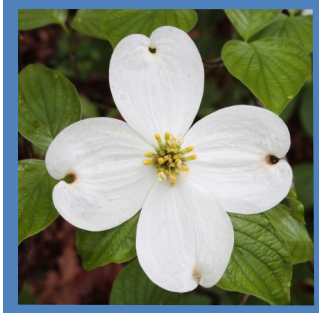


UNIVERSITY OF VIRGINIA

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 the University of Virginia as of and for the year ended June 30, 2016, and issued our report thereon, dated November 10, 2016. Our report, included in the University's basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.virginia.edu. Our audit of the 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 Aid performed in accordance with the U.S. Office of Management and Budget Uniform Guidance Compliance Supplement; and found no internal control findings requiring management's attention or instances of noncompliance required to be reported in relation to this testing.

–TABLE OF CONTENTS–

STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

Improve Virtual Private Network Security Controls

Applicable to: Academic Division

The University of Virginia (University) is making satisfactory 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. Best practices, such as the Special Publication 800-53r4 published by the National Institute for Standards and Technology, 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, 2016. 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 Controls for Granting and Restricting Elevated Workstation Privileges

Applicable to: Academic Division

The University is making satisfactory progress to address a weakness communicated in our prior year report in assigning and restricting elevated workstation privileges; however, corrective action remains in progress. The University tested an initial approach to resolve the weakness and identified several other potential solutions that, when implemented, should reduce this risk to a reasonable level. Additionally, as noted in the prior year, the University's corrective action should include the creation of policies and procedures to restrict and manage access to elevated workstation privileges in accordance with the University's adopted information security standard, ISO 27002:2013. Unnecessary privileges on workstations increase the risk that an end-user can unintentionally download and install malware on their computer.

The University plans to implement a solution and complete corrective action by August 20, 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 *my*VRS Navigator Reconciliation and Confirmation

Applicable to: Medical Center – repeat finding

The University of Virginia Medical Center (Medical Center) is not consistently reconciling information between the Virginia Retirement System's *my*VRS Navigator system and the Medical Center's PeopleSoft system, nor clearing retirement contribution data discrepancies between the two systems.

The Virginia Retirement System (VRS) Employer Manual, Contribution Confirmation and Payment Scheduling chapter, details the required tasks and roles of agencies in the reconciliation process. The process requires agencies to identify and correct errors prior to certifying payroll data monthly in *my*VRS Navigator. The Medical Center can obtain a Snapshot Download File from *my*VRS Navigator, which includes summary and detailed information for changes made to employee records since the last Snapshot. The manual requires a comparison of the Snapshot Download File to the Medical Center's payroll system to identify discrepancies and make corrections in either the payroll system or in *my*VRS Navigator, as necessary. Once the Medical Center completes the Snapshot reconciliation, confirmation of the Snapshot will post the information to the employee's record.

Failure to address data discrepancies between the two systems creates the risk for submission of inaccurate retirement contribution data and payment of incorrect contribution amounts for VRS-enrolled employees. As contributions are the basis for allocation of the Medical Center's share of the Commonwealth's net pension liability, inaccurate contributions can impact the accuracy of the financial statements. Difficulties in resolving discrepancies primarily relate to lack of access for medical center personnel to correct discrepancies for its employees, as the Academic Division performs this process on the Medical Center's behalf. Additionally, Medical Center personnel have not elevated concerns regarding lack of progress in addressing this issue to higher level management at the University resulting in significant delays in correcting the problems.

Medical Center management should work with representatives of the Academic Division to develop potential solutions to ensure proper entry and updating of information for Medical Center employees enrolled in the Virginia Retirement System. Potential solutions could include granting access to Medical Center employees to update information for Medical Center personnel or developing a memorandum of understanding between the Academic Division and Medical Center, which outlines roles and responsibilities for personnel in both divisions. Regardless, the solution must result in the appropriate reconciliation of information between *my*VRS Navigator and the Medical Center's systems, which includes the clearing of data discrepancies between systems in a timely manner.

Improve Security Awareness Training Program

Applicable to: Academic Division

The University does not have a process to monitor completion of security awareness training and enforce compliance with security awareness training requirements. The University's designated information security standard, ISO 27002:2013 (Security Standard), requires a security awareness training program that appropriately educates users about computer related risks, organizational policies, and data protection expectations.

Ten out of 50 University employees sampled (20 percent) did not complete the University's required security awareness training. Additionally, the most recent completion date for 33 of the employees tested (66 percent) occurred prior to July 1, 2015.

The Security Standard provides baseline security awareness training requirements, including the requirement for completion of the training on a periodic basis. The Security Standard emphasizes that training is not only for first time users, but for all users on a periodic basis, especially users who change positions or responsibilities. The Security Standard requires organizations to have a process for tracking the completion of the training and enforcement of the organizationally defined training requirements (*Security Standard, Section 7.2.2 Information security awareness, education and training*).

Ineffective security awareness training can increase the risk of security incidents that could result in legal, financial, or reputational damages. Untrained users are more likely to fall victim to common cyber-attacks, such as phishing or social engineering. Additionally, users who are not periodically trained on University data protection requirements may not fulfil their data protection responsibilities.

The University lacks an implemented policy that addresses these elements of the program. The University's current policy, the *Institutional Data Protection Standards version 1.1*, defines the requirement for the initial completion of the training, but does not include a requirement for additional periodic training. The policy does not include other program related requirements such as a process to track and enforce compliance or a requirement for additional role-based training for users who serve in technical or administrative roles. The University previously defined these requirements, including the requirement for annual completion of training, in a draft policy (*University Data Protection Standards version 2.0)*; however, this draft policy has not been formally approved to replace the previous version.

The University should update the relevant policy to include a requirement for periodic training completion, a requirement for additional role-based training, and a defined process to monitor completion and enforce compliance. The University should also implement and enforce compliance with the security awareness training program, so that all users complete training before

accessing University computer resources and on a periodic basis, thereby reducing data protection risk throughout the organization.

Improve and Comply with Sole Source Policies and Procedures

Applicable to: Academic Division

During fiscal year 2016, the Facilities Planning and Construction (FP&C) department did not procure certain sole source contracts in accordance with Attachment 1 to the University of Virginia's Management Agreement (the Procurement Rules), and the University of Virginia Higher Education Capital Outlay Manual (HECOM). For three out of five procurements reviewed (60 percent), FP&C used the sole source procurement method due to imminent deadlines imposed by requesting departments or because a department initiated preliminary procurement without consulting FP&C.

Per FP&C, timely notification of planned departmental construction activities is essential in providing adequate lead time for initiating competitive procurement as required by the Procurement Rules and the HECOM. As FP&C personnel did not receive timely notification of such activities, they did not have adequate time to consider competition to the extent practicable as required by Section 3 of the Procurement Rules and did not meet the criteria to utilize sole source procurement as defined in Section 5.E of the Procurement Rules and Section 11.10 of the HECOM. Failure to consider competition to the extent practicable can result in higher construction costs and questions regarding the appropriateness of contracts with certain businesses or contractors.

The University should implement procedures requiring departments to provide timely and adequate notification of the need for construction services to FP&C to allow for procurement of a contractor using a method allowed by the Procurement Rules and HECOM.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 10, 2016

The Honorable Terence R. McAuliffe
Governor of Virginia

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

Board of Visitors
University of Virginia

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 the **University of Virginia** 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 November 10, 2016. 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 Virtual Private Network Security Controls" and "Improve Controls for Granting and Restricting Elevated Workstation Privileges," which are described in the section titled "Status of Prior Year Findings and Recommendations," and "Improve *my*VRS Navigator Reconciliation and Confirmation," "Improve Security Awareness Training Program," and "Improve and Comply with Sole Source Policies and Procedures," 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 "Status of Prior Year Findings and Recommendations," in the findings entitled "Improve Virtual Private Network Security Controls," and "Improve Controls for Granting and Restricting Elevated Workstation Privileges," and in the section titled "Internal Control and Compliance Findings and Recommendations," in the findings entitled "Improve Security Awareness Training Program," and "Improve and Comply with Sole Source Policies and Procedures."

The University's Response to Findings

We discussed this report with management at an exit conference held on November 2, 2016. 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 made progress in addressing the previously reported findings "Improve Virtual Private Network Security Controls" and "Improve Controls for Granting and Restricting Elevated Workstation Privileges," but has not completed implementation of its corrective action plan for each finding. Accordingly, we included these findings in the section entitled "Status of Prior Year Findings and Recommendations."

The University's Medical Center has not taken adequate corrective action with respect to the previously reported finding "Improve *my*VRS Navigator Reconciliation and Confirmation." Accordingly, we included this finding 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

EMS/clj

Improve myVRS Navigator Reconciliation and Confirmation
Applicable to: Medical Center – repeat finding

University Response:

The University of Virginia Medical Center concurs with the APA's finding.

Responsible for Corrective Action: Kim Holdren, UVA Medical Center Controller

Anticipated Completion Date: November 2016

Corrective Action to be taken by University Management:

In response to this finding, the Medical Center Payroll Office met with the Director of Benefits for UVA, on 10/11/16 to discuss the challenges with reconciling the activity. Specifically, it was determined that the Medical Center did not have the appropriate access for the new payroll manager and did not have processes in place to reconcile the activity. As of November 2016, the access has been provided and the processes designed. Medical Center management has identified the reconciling items between VRS and the Payroll System for the fiscal year ended 6/30/16, as well as for the month ended 10/31/16. In addition, management has documented the steps being taken to resolve each of the reconciling items and expects VRS to update their system accordingly. At this point, the Medical Center is current on its reconciliation requirements.

Improve Security Awareness Training Program
Applicable to: Academic Division

University Response:

Regarding the recommendation to improve our Security Awareness Training Program, the University concurs with the recommendation and will take the corrective actions listed below.

Responsible for Corrective Action:
Virginia H. Evans, Chief Information Officer
Jason C. Belford, Chief Information Security Officer

Anticipated Completion Date: December 29, 2017

Corrective Action to be taken by University Management:

The University will:

- Update existing policies to address periodic security training and ensure that additional role-based training is included and
- Implement a process to monitor completions and enforce compliance.

As part of the SecureUVA program (formerly named the Security Enhancement Program), the University will update all IT security policies, standards, and guidelines. The requirement for security training, as well as more periodic training updates, will be covered in these updated standards. This project has started and will be completed by **June 30, 2017**. The university will also develop methods to track and enforce compliance as part of a second SecureUVA project. This project will be scoped to update the current training materials and training system, which will help track and enforce training requirements. This project is scheduled to begin in March 2017 and will be completed by **December 29, 2017**.

Improve and Comply with Sole Source Policies and Procedures
Applicable to: Academic Division

University Response:

For the three sole sources procurements cited, the University believes that it has chosen the correct procurement method based on the situation, and understands the need for careful consideration of schedule criteria as a basis for sole source procurement. The University considers the project timeline to be a critical component in the process of selecting a procurement method and contractor, and in successfully achieving the mission of the institution. Facilities Planning & Construction (FP&C) does commit to better educating internal clients about the HECOM requirements with respect to sole source and competitive procurements are addressed. FP&C will initiate increased scrutiny of any future sole source requests with the end goal being to maximize competitive procurements to the extent practicable and consistent with relevant sections of the law.

Responsible for Corrective Action:
Jeff Moore, Director of Construction Services & Contract Administration

Anticipated Completion Date: March 31, 2017

Corrective Action to be taken by University Management:

- University Contracting Officer, Associate Vice President-Chief Facilities Officer will provide clear and direct communication to emphasize the importance of compliance with UVa Procurement Rules and Sole Source Policies and Procedures.
- Facilities Planning & Construction (FP&C) will provide online resources, email notifications, and in person communications with the University community between now and March 31, 2017 to convey the State Procurement Rules and the UVA HECOM requirements for Sole Source procurements, procurement best practices, and the benefits of and time required for competitive procurements including:
  - Timely notification of planned departmental construction activities is essential in providing adequate lead time for initiating competitive procurement.
  - Imminent deadlines imposed by requesting clients, or clients initiating preliminary procurement without consulting FP&C, are not currently recognized justifications for Sole Source procurement by APA.
  - The AVP & CFO is the authority acting as the UVA contracting officer, and Sole Source approval is based on his judgment on specific procurements.
- FP&C will implement procedures requiring clients to provide timely and adequate notification of the need for construction services to FP&C to allow for procurement of a contractor using a method allowed by the Procurement Rules and HECOM.
- FP&C will initiate increased scrutiny of future Sole Source requests with the end goal being to maximize competitive procurements to the extent practicable and consistent with relevant sections of the law.

UNIVERSITY OF VIRGINIA

As of June 30, 2016

BOARD OF VISITORS

William H. Goodwin, Jr.
Rector

Frank M. Conner, III
Vice Rector

Frank B. Atkinson
Mark T. Bowles
L.D. Britt
Whittington W. Clement
Helen E. Dragas
Kevin J. Fay
Barbara J. Fried
Frank E. Genovese
John A. Griffin
Victoria D. Harker
Bobbie G. Kilberg
John G. Macfarlane, III
Tammy S. Murphy
James V. Reyes
Jeffrey C. Walker

Phoebe A. Willis
Student Representative

Joe Garofalo
Faculty Representative

Susan G. Harris
Secretary to the Board of Visitors

ADMINISTRATIVE OFFICERS

Teresa A. Sullivan
President

Patrick D. Hogan
Executive Vice President and Chief Operating Officer