UNIVERSITY OF VIRGINIA

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 the University of Virginia as of and for the year ended June 30, 2017, and issued our report thereon, dated November 7, 2017. Our report is included in the University's basic financial statements that it anticipates releasing on or around December 7, 2017. 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 or other matters required to be reported under Government Auditing Standards.

Our audit also included testing over the major federal program of the Research and Development Cluster for the Commonwealth's Single Audit as described in the U.S. Office of Management and Budget Compliance Supplement; and found no internal control findings requiring management's attention or instances of noncompliance in relation to this testing.

–TABLE OF CONTENTS–

STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

Improve Controls for Granting and Restricting Elevated Workstations Privileges
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial with satisfactory progress

The University of Virginia's Academic Division (Academic Division) is making satisfactory progress to address the information security weakness communicated in our prior year audit report regarding assigning, restricting, and tracking elevated workstation privileges; however, corrective action remains in progress. The Academic Division created a standard operating procedure as interim guidance for granting and restricting elevated workstation privileges, which includes the controls required by its adopted information security standard, ISO 27002. The Academic Division distributed the interim guidance to its departments and plans to integrate it into new policies and standards. The Academic Division is requiring departments to comply by March 2018. The fiscal year 2018 audit will include an evaluation of the completed corrective action and determine whether the Academic Division satisfactorily resolved the weakness.

Improve Security Awareness Training Program
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial with satisfactory progress

The Academic Division is making satisfactory progress to address an information security weakness communicated in our prior year audit report regarding improving the security awareness training program; however, corrective action remains in progress. Specifically, the Academic Division has developed policies to address security awareness training requirements; however, it has not yet implemented the policies. The Academic Division also created a project charter that, when implemented, will assign the Chief Information Security Officer with security awareness training oversight and will implement a process whereby it can monitor completion and enforce compliance with security awareness training requirements.

The Academic Division plans to complete the project by December 2017. The fiscal year 2018 audit will include an evaluation of the completed corrective action and determine whether the Academic Division satisfactorily resolved the weakness.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Database Security
Applicable to: Medical Center
Type: Internal Control and Compliance
Severity: Significant Deficiency

The University of Virginia Medical Center (Medical Center) does not implement some of the required controls to protect the database management system (database) platform that supports the primary patient record and billing system. The Medical Center's adopted information security standard, NIST SP800-53 (Security Standard), and industry best practices, such as the Department of Defense's Security Technical Implementation Guides, prescribe several required and recommended security controls to safeguard systems that contain or process sensitive data.

The Security Standard and best practices require and recommend implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability. We identified eight controls that the Medical Center does not implement that are generally related to access and baseline configuration management. We communicated these specific control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under §2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Without enforcing proper access and baseline configuration management controls for the system, the Medical Center increases the data security risk associated with the sensitive and financial transactions processed by the system. These findings increase the risk of a data breach or system unavailability, which could lead to financial, legal, regulatory, and reputational damages.

The Medical Center should dedicate the necessary resources to configure appropriate security controls for the database in accordance with the Security Standard and best practices. Implementing these controls will help maintain the confidentiality, availability, and integrity of the sensitive and mission critical data stored or processed in the database.

Improve IT Risk Management Process and Documentation
Applicable to: Medical Center
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Medical Center's information technology (IT) risk management documentation is incomplete and does not include certain attributes that the Medical Center needs to effectively evaluate and implement necessary information security controls.

The Security Standard provides a structured approach to IT risk management that includes the identification and evaluation of several attributes. Upon review of the Medical Center's IT risk management process and documentation, the Medical Center did not evaluate the following attributes across all IT systems as part of their risk management process:

- Identifying mission essential functions and supporting business functions;
- Prioritizing mission essential functions;
- Assigning recovery time objectives for each mission essential function;
- Identifying information systems supporting each mission essential function;
- Identifying data types handled by each system classified as sensitive; and
- Creating risk assessments for each system classified as sensitive.

  (Security Standard sections: CP-2 Contingency Plan, 3.1 Selecting Security Control Baselines, RA-2 Security Categorization, and RA-3 Risk Assessment.)

The Medical Center may not be able to restore or protect sensitive systems in accordance with management's expectations if the Medical Center does not incorporate these attributes into the IT risk management process. The Medical Center's risk management documentation is incomplete because its risk management process does not adequately consider all of the elements defined by the Security Standard. Additionally, the Medical Center postponed completing risk assessments for two sensitive systems due to projects to acquire and implement additional technical resources. The Medical Center should incorporate the attributes described above, which will reduce the risk of failing to classify a system appropriately and protect it according to its sensitivity classification.

Improve Oversight of Third Party Service Providers
Applicable to: Medical Center
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Medical Center does not have a sufficient process for gaining ongoing external assurance that third-party service providers have adequate security controls to protect the Medical Center's IT environment and sensitive data in accordance with organizational policies and the Security Standard. The Medical Center outsources certain business tasks and functions to service providers who transmit, process, or store sensitive Medical Center data.

The Security Standard recognizes that organizations may procure IT equipment, systems, or services from third-party service providers and states that organizations must ensure that such providers meet the organization's established security requirements. The Security Standard requires that organizations define and employ processes to monitor security control compliance by external service providers on an ongoing basis (Security Standard section: SA-9 External Information System Services). By not defining and employing a process to gain periodic assurance over third-party service providers' internal controls, the Medical Center cannot validate that the provider has effective IT controls to protect the Medical Center's IT environment and sensitive data in accordance with organizational policies, state and federal regulations, and the Security Standard.

The Medical Center does not gain ongoing external assurance over third-party service providers' IT environments because they do not define a formal process in their information security program for identifying procured third-party service provider contracts and providing appropriate oversight. During the procurement process for cloud-based vendors, the Medical Center requests a self-reported cloud risk assessment over security controls from each potential cloud-based vendor to collect information to use during contract negotiations. However, after completing a vendor contract, the Medical Center does not have a defined process for obtaining and evaluating forms of external assurance on a periodic basis from either physical or cloud-based vendors that provide technology and information security services.

The Medical Center should develop a formal process for obtaining and evaluating forms of external assurance over third-party service providers' security controls on an ongoing basis to ensure that the security controls comply with organizational policies and the Security Standard to protect the Medical Center's IT environment and sensitive data. One way to gain reasonable assurance is by requesting, reviewing, and evaluating Service Organization Control reports issued by independent third-party assurance organizations. After the Medical Center defines a formal process for ongoing service provider oversight, they should employ it into their information security program.

Improve Monitoring over Estimated Accounts Payable

Applicable to: Medical Center
Type: Internal Control
Severity: Significant Deficiency

The Medical Center is not adequately reviewing and monitoring manual accounts payable accruals resulting in an overstatement of accounts payable and accrued expenses in the financial statements. Audit testing over the Medical Center's account summary and reconciliation, which reconciles $6,600,256 in manual accounts payable entries, uncovered three items totaling $2,169,988 that lacked adequate support and which the Medical Center improperly included as accruals for fiscal year 2017. Medical Center personnel originally posted these accruals in fiscal year 2013 and fiscal year 2015.

The Medical Center's current reconciliation process is inadequate for ensuring proper reversal of accrual entries in the manual accounts payable account during the next fiscal year or when the Medical Center pays the related invoice. The primary composition of this account is estimates for invoices not received at year-end, which the Medical Center records by journal entry. There is no control in place to flag related invoices when received and remove the estimated payables from the manual accounts payable account when paid.

All invoices received by the Medical Center flow to the Accounts Payable Department, and an invoice accrued in the manual accounts payable account could flow through the Accounts Payable Department with no notice to the individual recording the original journal entry. As a result, the person who made the journal entry would have no knowledge that the Medical Center received and paid the invoice and would not know to reverse the estimated payable. Lacking this knowledge, if Accounts Payable received invoices related to these estimated payables in July or August, there is risk that the

Medical Center may accrue the invoice as an account payable based on the date it received the good or service and double count the payable in the financial statements.

The Medical Center should improve its reconciliation process for the manual accounts payable account by maintaining detailed support for these entries and tracking estimated payables to reverse in the next period. Medical Center personnel should review all entries older than one year to evaluate whether the estimate of the amount payable remains accurate or needs revision or to ensure proper liquidation of the payable once paid.

Improve Policies and Procedures for Removal of Terminated Employee Badge Access
Applicable to: Medical Center
Type: Internal Control
Severity: Significant Deficiency

The Medical Center does not have adequate documentation supporting badge access removal for employees separating from the Medical Center. For 12 out of 19 employees tested (63 percent), the last modified date for the employee badge was more than one month after the employee's termination date, and the Medical Center could not provide additional evidence to show that it collected the badge or removed the employees' badge access in a timely manner. In addition, current written policies are not adequate to provide for timely removal of employee badge access when employees leave the Medical Center.

The ID badge system does not have the capability to show historical information regarding employee badge access activation or removal. The current system only records a last modified date for the employee badge ID, and not an employee badge ID termination date. This current construct does not allow the Medical Center Badge ID office to provide adequate and reasonable evidence that an employee's badge ID access terminated with an employee's employment termination date. Untimely badge access removal increases the risk that terminated employees maintain access to restricted areas of the Medical Center and/or sensitive information.

The Medical Center should develop policies and procedures to provide for timely deactivation of employee badge access, and should maintain documentation as evidence of the date of deactivation.

Improve Terminated Employee Procedures
Applicable to: Academic Division
Type: Internal Control
Severity: Significant Deficiency

Departments are not sufficiently completing off-boarding checklists for employees terminating employment with the Academic Division of the University of Virginia. For the sample selected, 16 of 46 employees (35 percent) did not properly complete the required off-boarding checklist.

Academic Division terminated employee procedures, for both staff employees and faculty members, require a completed off-boarding checklist to officially separate from the University.

However, the off-boarding procedures for both staff and faculty do not define a specific timeframe for completing the off-boarding checklist. These procedures also do not specify all specific employee types requiring a checklist (e.g. temporary employees). As a result, many departments were not aware a checklist was required.

Inadequate processing of terminated employees can result in potential overpayments to former employees and delays in removing access to property, information systems, and potentially sensitive information. The Office of Human Resource Management and Provost Office should review current procedures for processing terminations to ensure accurate and timely completion of all off-boarding checklists. Management should consider revising staff and faculty off-boarding procedures to include a clearly defined timeframe for completing the off-boarding checklist after the termination date of an employee. Academic Division management should reinforce the importance of completing off-boarding checklists accurately and timely to alleviate the potential for future risk.

Comply with Commonwealth Requirements for Wage Employees

Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Academic Division should improve its process for monitoring non-benefit employee work hours to ensure compliance with Chapter 836 §4-7.01g of the 2017 Virginia Acts of Assembly. The University is responsible for implementing policies and procedures to ensure employees who are not eligible for benefits do not work more than 29 hours per week on average over a 12-month period (the requirement). The Academic Division has policies and procedures in place to monitor this, but current procedures do not prevent departments from allowing an employee to exceed the requirement. In a review of all non-benefit employees who worked during the measurement period of October 3, 2015, to October 2, 2016, 10 employees exceeded the requirement.

For certain Commonwealth employees, Chapter 836 §4-7.01g of the 2017 Virginia Acts of Assembly requires that they may not work more than 29 hours per week on average over a twelve month period. To implement this requirement, Human Resource Policy 2.20, developed by the Commonwealth's Department of Human Resource Management, states that wage employees are limited to working 1,500 hours per agency per year. The Commonwealth developed this policy to ensure compliance with the requirements of the Patient Protection and Affordable Care Act, which requires employers to provide health benefits to certain employees and could bring penalties for noncompliance.

To avoid penalty payments and ensure compliance with state and federal requirements, the Office of Human Resource Management should reinforce to departments and employees the importance of not exceeding the annual hour requirement. This includes not allowing employees who have reached the limit to work again until the beginning of the next measurement period.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 7, 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
The 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, 2017, and the related notes to the financial statements, which collectively comprise the University of Virginia's basic financial statements and have issued our report thereon dated November 7, 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 of Virginia, 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 of Virginia'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 of Virginia's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University of Virginia'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 Controls for Granting and Restricting Elevated Workstation Privileges" and "Improve Security Awareness Training Program," which are described in the section titled "Status of Prior Year Findings and Recommendations" and deficiencies entitled "Improve Database Security," "Improve IT Risk Management Process and Documentation," "Improve Oversight of Third Party Service Providers," "Improve Monitoring over Estimated Accounts Payable," "Improve Policies and Procedures for Removal of Terminated Employee Badge Access," "Improve Terminated Employee Procedures," and "Comply with Commonwealth Requirements for Wage Employees," 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 sections titled "Status of Prior Year Findings and Recommendations" and "Internal Control and Compliance Findings and Recommendations" in the findings entitled "Improve Controls for Granting and Restricting Elevated Workstation Privileges," "Improve Security Awareness Training Program," "Improve Database Security," "Improve IT Risk Management Process and Documentation," "Improve Oversight of Third Party Service Providers," and "Comply with Commonwealth Requirements for Wage Employees."

The University's Response to Findings

We discussed this report with management at an exit conference held on November 9, 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 implemented corrective action with respect to the previously reported findings “Improve Controls for Granting and Restricting Elevated Workstation Privileges” and “Improve Security Awareness Training Program.” Accordingly, we included these findings in the section entitled “Status of Prior Year 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/alh

Improve Database Security
Applicable to: Medical Center

University Response:
The UVA Medical Center concurs with APA's finding.

Responsible for Corrective Action: Erin Trost, Interim IT Security Director/Senior IT Security Analyst

Anticipated Completion Date: July 1, 2018

Corrective Action to be taken by University Management:
The APA audited the database and noted eight areas of improvement. Two of the eight areas related to access management and were fixed immediately upon notification from the APA. The APA was notified these had been addressed. The remaining six areas noted are related specifically to the configurations prepackaged by the vendor. The UVA Medical Center has been actively working with the vendor in order to determine if remediation is possible and within the ability of the database to control. The issue is not unique to UVA.

Improve IT Risk Management Process and Documentation
Applicable to: Medical Center

University Response:
The UVA Medical Center concurs with APA's finding.

Responsible for Corrective Action: Erin Trost, Interim IT Security Director/Senior IT Security Analyst

Anticipated Completion Date: June, 2018; December, 2018

Corrective Action to be taken by University Management:
The UVA Medical Center (UVAMC) has a comprehensive and well defined Business Continuity Plan and Disaster Recovery Plan (BCP/DR). Included in the BCP/DR is the Business Impact Analysis. UVAMC started a project near the end of fiscal year 2017 to review the current Business Impact Analysis and determine where there might be gaps related to standards listed in NIST 800-34 Contingency Planning Guide for Federal Systems. The UVAMC has plans to complete this gap analysis by 06/30/2018.

UVAMC completed the annual risk assessment for the system in March 2017. Due to the timing of the go-live and the migration of certain HR systems, UVAMC made a deliberate decision to defer assessments of risk for functions covered by certain vendors. Both risk assessments are set to be completed in the upcoming year (2018), which is still within the window of compliance.

Improve Oversight of Third Party Service Providers
Applicable to: Medical Center

University Response:
The UVA Medical Center concurs with APA's finding.

Responsible for Corrective Action: Erin Trost, Interim IT Security Director/Senior IT Security Analyst

Anticipated Completion Date: July 1, 2018

Corrective Action to be taken by University Management:
The UVA Medical Center (UVAMC) has developed a comprehensive risk management and assessment framework that applies to third-party vendors. The risk assessment process is a collaborative endeavor involving UVAMC IT Security, Procurement, Clinical Engineering, and Senior Leadership. For third-party vendors, one of the following risk assessments need to be completed: Cloud Risk Assessment, Black Box Risk Assessment, Medical Device Risk Assessment, and Security/Exhibit Requirements. In addition, UVAMC created an annual review process for the storage vendor, as well as a process to review risk assessments when a contract is up for renewal. UVAMC will develop a review process that clearly exhibits and documents adherence of third parties to UVAMC defined standards and controls.

Improve Monitoring over Estimated Accounts Payable
Applicable to: Medical Center

University Response:
The UVA Medical Center concurs with APA's finding.

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

Anticipated Completion Date: Completed 09/30/2017

Corrective Action to be taken by University Management:
The UVA Medical Center reconciles this account every month. In addition to the monthly reconciliation of this account, highlighting the components, an additional vendor query will be run against the accounts payable account to either further substantiate the need for the accrual, or to verify the accrual needs to be reversed. The two accruals noted were an oversight during the reconciliation process.

Improve Policies and Procedures for Removal of Terminated Employee Badge Access
Applicable to: Medical Center

University Response:
The UVA Medical Center concurs with APA's finding.

Responsible for Corrective Action: David Cornelius, Security Systems Manager

Anticipated Completion Date: Completed 09/30/2017

Corrective Action to be taken by University Management:
The UVA Medical Center will implement a new policy, termination of team member badges, that upon notification from Medical Center computing, the ID Badge office has 24 hours to terminate the badge in the system. In addition, to electronically document the termination date of the employee's badge, the date will be entered into the Expiration field in the ID badge system. Per system logs, of the 19 terminated employees tested, none of them used their badges post the termination date.

Improve Terminated Employee Procedures
Applicable to: Academic Division

University Response:

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

Responsible for Corrective Action: Adam Weikel, Assistant Vice President for Service

Anticipated Completion Date: July 1, 2018

Corrective Action to be taken by University Management:
The current employee off-boarding process is a paper-based, manual process, dependent on hiring unit implementation, collection of signatures, and limited technology. The University is in the process of implementing a new HR Management System for future state employee transaction management and engagement. Additional refinement of off-boarding procedures, inclusive of timeframes for completion, and impacted employee populations, are planned as part of this project. The off-boarding process will be significantly enhanced as an element of the new HR Management System's process capacity, resulting in improvement in compliance with University off boarding procedures.

Until the new HR Management System and off-boarding process can be implemented, Human Resources and Provost Office will revisit terminated employee procedures and define a specific timeframe for completing the off-boarding checklist, as well as identify all employee types requiring an off-boarding checklist. The revised procedures will be clearly communicated to all departments. In addition, the University will continue to perform random audits to evaluate compliance with the off-boarding toolkit.

Comply with Commonwealth Requirements for Wage Employees

Applicable to: Academic Division

University Response:

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

Responsible for Corrective Action: John Kosky, Assistant Vice President for IMPACT and Decision Support

Anticipated Completion Date: July 1, 2018

Corrective Action to be taken by University Management:

The Human Resource department will reinforce Human Resource Policy 2.20 and the 1,500 hour rule to all departments. In addition, Payroll/Human Resources will implement additional controls to monitor non-benefit employees' hours and communicate employees approaching the annual limit to the respective department in a timely manner.

In addition, the University is in the process of implementing a new HR management system, which will enable a more rigorous process to ensure termination takes place before the 1,500 hour threshold.

UNIVERSITY OF VIRGINIA

As of June 30, 2017

BOARD OF VISITORS

William H. Goodwin, Jr.
Rector

Frank M. Conner, III
Vice Rector

Mark T. Bowles
L.D. Britt
Whittington W. Clement
Elizabeth M. Cranwell
Thomas A. DePasquale
Kevin J. Fay
Barbara J. Fried
Frank E. Genovese
John A. Griffin
Babur B. Lateef
John G. Macfarlane, III
Tammy S. Murphy
James B. Murray, Jr.
James V. Reyes
Jeffrey C. Walker

Bryanna F. Miller
Student Representative

Nina J. Solenski
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