UNIVERSITY OF VIRGINIA

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2018

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, 2018, and issued our report thereon, dated November 27, 2018. Our report is included in the University's basic financial statements that it anticipates releasing on or around December 6, 2018. Our audit found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; 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 performed in accordance with the U.S. Office of Management and Budget Compliance Supplement Part 5 Student Financial Assistance Programs; and found internal control findings requiring management's attention and instances of noncompliance in relation to this testing.

–TABLE OF CONTENTS–

STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

Improve Security Awareness Training Program
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2016, with satisfactory progress in this area)

The University of Virginia Academic Division (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 established a new policy addressing security awareness training requirements, including a requirement that employees must complete annual security awareness training. The Academic Division will provide training, track completion and enforce policy requirements in its new learning management system (LMS), which it anticipates going into production in January 2019.

However, the new policy does not require that newly hired employees must complete the training prior to receiving access rights to the Academic Division's information technology (IT) systems, and the Academic Division does not document the process used to track and enforce organizationally defined training requirements in an accompanying procedure.

The Academic Division's adopted information security standard, ISO 27002 (Academic Division Security Standard), section 7.2.2, requires that organizations provide training for all users on a regular basis and that organizations provide initial training to both employees transferring to new positions, as well as to new employees, before the role becomes active. The Academic Division Security Standard additionally requires organizations to ensure effective security awareness training by enforcing and assessing training completion. Ineffective security awareness training increases the risk of security incidents related to untrained users falling victim to common cyber-attacks, such as phishing or social engineering.

The Academic Division plans to incorporate annual security awareness training into the new LMS, including integrating the process of monitoring and tracking at-hire and annual security awareness training completion within the LMS. The fiscal year 2019 audit will include an evaluation of the Academic Division's completed corrective action and determine whether the Academic Division satisfactorily resolved the weakness.

Improve IT Risk Management Process and Documentation

Applicable to: Medical Center
Type of Finding: Internal Control and Compliance
Severity of Deficiency: Significant Deficiency
Repeat: Yes (first issued in 2017, with satisfactory progress in this area)

The University of Virginia Medical Center (Medical Center) continues to implement their corrective action plan to address the weakness communicated in our prior year audit report to improve risk management processes and supporting documentation. The Medical Center began a project in May 2018 to ensure its risk management process and procedures address all required elements in its adopted information security standard, NIST 800-53 (Medical Center Security Standard). Thus far, the Medical Center has complete risk assessments for several of its mission critical systems and has draft versions of its risk management documents.

The Medical Center plans to complete and approve all risk management documents by January 2019. The fiscal year 2019 audit will include an evaluation of the Medical Center's complete risk management documents to determine if they are adequate to resolve the weakness.

Improve Oversight of Third-Party Service Providers

Applicable to: Medical Center
Type of Finding: Internal Control and Compliance
Severity of Deficiency: Significant Deficiency
Repeat: Yes (first issued in 2017, with limited progress in this area)

The Medical Center continues to address the information security weakness communicated in our prior year audit report to gain assurance their third-party providers have secure IT environments to protect sensitive and mission critical data. Third-party providers are organizations that perform outsourced business tasks or functions on behalf of the Medical Center. The Medical Center uses six third-party providers that transmit, process, or store sensitive and mission critical data.

The Medical Center does not have an effective formal, documented policy, procedure, and process to continuously manage their third party providers. To gain assurance over provider controls, the Medical Center receives self-reported information security documentation from its third-party providers. The Medical Center reviews the information and assigns a risk level, but IT staff does not obtain confirmation of the accuracy of the information provided, either through direct review of the organization's controls or external validation of the information by an independent organization.

The Medical Center Security Standard, section SA-9, requires that organizations define and employ processes to monitor security control compliance by external service providers on an ongoing basis. By not gaining adequate assurance over third-party service providers' IT environments, the Medical Center cannot validate the effectiveness of the providers' IT controls to protect its sensitive and mission critical data.

The Medical Center should develop a formal process to gain ongoing assurance that its third-party providers have secure IT environments to protect sensitive and mission critical data. To do this, the Medical Center should perform an annual security audit of the provider's IT environment or review independent audit reports, such as System and Organization Controls (SOC) reports, on an annual basis. After the Medical Center develops a formal process, they should incorporate it into their information security program. The fiscal year 2019 audit will include an evaluation of the Medical Center's process to gain assurance over third-party providers and determine whether it is sufficient to resolve the weakness.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Oversight of Third-Party Service Providers
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The Academic Division does not gain assurance that IT-related third-party service providers who create, obtain, transmit, use, maintain, process, or dispose of University data have secure IT environments to protect sensitive and mission critical data. Third-party providers are organizations that perform outsourced business tasks or functions on behalf of the Academic Division. The Academic Division uses seven IT service providers that transmit, process, or store sensitive and mission critical data.

The Academic Division has a process in place to manage these third-party providers, but has not performed regular security audits of the provider's IT environment or reviewed independent audit reports, such as SOC reports, on a regular basis to determine that agreed upon security controls are in place and operating effectively.

For any contracts with vendors that may access, process, store, communicate, or provide IT infrastructure components, the Academic Division requires the vendor to complete a data protection addendum wherein the vendor agrees to adhere to certain security requirements. The addendum states that Academic Division personnel have the right to conduct audits of the vendor at any time, and that the vendor must conduct, or have conducted, an annual independent security audit that attests to the vendor's security policies, procedures, and controls. The addendum further states that the vendor must provide the results of independent security audits at the Academic Division's request, and that the vendor must modify its security measures, based on the results of the audit, to meet the controls agreed upon in the addendum. However, the Academic Division has not requested and evaluated the results of independent security audits for any of its third-party providers.

The Academic Division Security Standard requires that organizations regularly monitor, review, and audit vendor services to ensure the third-party vendors adhere to the information security terms

and conditions of the agreements. By not gaining adequate assurance over third-party service providers' IT environments, the Academic Division cannot validate the effectiveness of the providers' IT controls to protect the Academic Division's sensitive and mission critical data.

The Academic Division did not gain assurance over these IT-related third-party providers' IT environments, because it did not follow-through with requesting the results of each vendor's independent security audit, which the terms of the contract addendum require. The Academic Division recently began the process of obtaining and reviewing SOC reports from the vendors.

The Academic Division should gain assurance that each of their IT-related third-party providers have secure IT environments to protect sensitive and mission critical data. To do this, the Academic Division should perform an annual security audit of the provider's IT environment, or obtain and evaluate SOC reports, or other independent audit reports, to confirm that each provider maintains effective IT controls to protect its sensitive and mission critical data.

Improve Database Security
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The Academic Division does not implement some required controls to protect the database management system (database) platform that supports the student record keeping and billing system. The Academic Division Security Standard, and industry best practices, such as the Center for Internet Security's Benchmark (CIS Benchmark), prescribe several required and recommended security controls to safeguard systems that contain or process sensitive data.

We identified fourteen controls that the Academic Division 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.

Not meeting the minimum requirements in the Academic Division Security Standard and aligning the database's settings and configurations with industry best practices may reduce the effectiveness of the Academic Division's objective to protect data within the database.

The Academic Division should address the risks present in the database and develop a database hardening process to ensure configurations and controls align with the Academic Division Security Standard and industry best practices. Implementing these processes and controls will help maintain the confidentiality, integrity, and availability of Academic Division data and meet the requirements defined in the Academic Division Security Standard.

Improve Revenue Recognition for Non-reimbursement Grants
Applicable to: Academic Division
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

The Academic Division improperly recognized revenue related to non-reimbursable grants and contracts, which overstated unearned revenue and understated revenue in prior periods. Based on GASB Codification section 1600.103, resources resulting from exchange and exchange-like transactions should be recognized as revenue when an exchange takes place. Financial statement preparers should recognize revenue related to nonexchange transactions in accordance with GASB Codification N50, which requires a recipient to meet certain timing and eligibility criteria before recognizing revenue.

The Academic Division's accounting and financial reporting system includes automatic accounting rules that recognize revenue for expenditure-driven or reimbursement-based grants as the Academic Division posts expenses to the grants. However, the system treats other types of grants, where grantors provide resources through fixed payments or where the Academic Division receives funding on a per participant basis, in the same manner, resulting in a delay in the recognition of revenue. These grants do not require repayment of unused funds or include additional eligibility or timing criteria, which allows for recognition of the resources as revenue when received. Due to the improperly designed control within the accounting and financial reporting system, the Academic Division misstated the prior years' financial statements, resulting in the need to record a $21.5 million increase to beginning net position and $6.8 million increase in grants and contracts revenue for fiscal year 2018.

The Academic Division financial reporting team worked with the Office of Sponsored Programs to identify the extent of the issue and addressed the problem by creating a process to properly recognize certain grant revenue in the financial statements. The Academic Division should formalize this process in its financial reporting policies and procedures to ensure proper accounting for the revenue generated by certain non-reimbursable grants during future fiscal years.

Improve Notification Process for Federal Direct Loan Awards to Students
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The Academic Division Student Financial Services office (Student Financial Services) did not properly notify students awarded Federal Direct Loans for two of 25 students (8%) tested. Upon further review, Student Financial Services determined 499 of the 6,522 students (7.6%) receiving Federal Direct Loans did not receive required loan notifications. The Code of Federal Regulations requires written award notifications to students, which include important details on the rights, options, and requirements of the student loan. Student Financial Services uses an automated system to send the required notifications to students. Due to a programming error, the automated system did not capture certain

types of loan disbursement transactions and, as a result, the Student Financial Services office did not provide the notifications to these students.

Code of Federal Regulations, 34 CFR §668.165(a) (2), requires institutions to properly notify students receiving Federal Direct Loans, in writing, of the date and amount of the disbursement, the student's right to cancel all or a portion of a loan or loan disbursement, and the procedure and time by which the student must notify the institution that he or she wishes to cancel the loan. Failure to properly notify students in accordance with Federal Regulations may result in fines, withholding of Title IV funds, or suspension or termination of participation in Title IV programs.

The Student Financial Services office should revisit the system programming that triggers the loan notification process to ensure the Academic Division properly notifies all students who receive Federal Direct Loans as required by the Code of Federal Regulations.

Promptly Return Title IV Funds
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The financial aid offices at the University of Virginia's medical and law schools (the schools) did not promptly return Title IV funds within 45 days of the institution's determination that a student withdrew. For four of eight students (50%) withdrawing from the schools during the academic year, the schools returned the funds between 56 and 67 days following the determination the student withdrew from the university. The medical and law schools have separate financial aid offices, which handle any necessary return to Title IV calculations and the returning of Title IV funds to the Department of Education. Representatives from the schools indicated limited staff during the year led to the delay in returning the funds.

Code of Federal Regulations, 34 CFR §668.22, states when a recipient of Title IV grant or loan assistance withdraws from an institution during a period of enrollment in which the recipient began attendance, the institution must determine the amount of Title IV grant or loan assistance that the student earned as of the student's withdrawal date and return the money within a reasonable timeframe. The institution must return unearned funds within 45 days after the date that the institution determines the student has withdrawn. Failure to comply with the return provisions of the Code of Federal Regulations could result in the initiation of an adverse action by the Department of Education.

The financial aid offices within the medical and law schools should review their policies and procedures and amend current processes to enable prompt return of Title IV funds to the Department of Education within the prescribed 45-day timeframe.

Improve Reporting to the National Student Loan Data System
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Academic Division personnel did not report enrollment data to the National Student Loan Data System (NSLDS) accurately and timely. In three of 12 student withdrawals (25%) tested, the Academic Division reported an incorrect effective enrollment status date and did not report the change in enrollment status timely. We did not identify noncompliance in a sample of 25 graduating students tested.

In accordance with Code of Federal Regulations 34 CFR 685.309, and further outlined in the NSLDS Enrollment Guide, published by the Department of Education, enrollment changes must be reported to NSLDS within 30 days when attendance changes, unless a roster file will be submitted within 60 days. The accuracy of Title IV enrollment data depends heavily on information reported by institutions. Untimely and inaccurate data submission to NSLDS can affect the reliance placed on the system by the Department of Education for monitoring purposes and other higher education institutions when making aid decisions. Noncompliance may also have implication on an institution's participation in Title IV programs and can potentially impact loan repayment grace periods. Procedural delays in approving withdrawal applications appear to have contributed to delays in submitting timely information to NSLDS; however, the cause underlying the submission of inaccurate information is indeterminate.

Management should perform a comprehensive review of current enrollment reporting policies and procedures to improve timeliness of submissions to NSLDS. Management should implement corrective action to prevent future noncompliance and should consider implementing a quality control review process to monitor the accuracy of submitted enrollment batches.

Improve Wireless Local Area Network Security
Applicable to: Medical Center
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The Medical Center does not secure the agency's wireless local area network (WLAN) with some of the minimum security controls required by the Medical Center Security Standard. The Medical Center manages and maintains its own wireless network and relies on the WLAN to provide various levels of access to protected resources.

We identified controls that the Medical Center does not implement that are generally related to patch management, authentication, transmission confidentiality and integrity, and access control. 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.

A lack of sufficient policies, procedures, and hardening guidelines contributes to the weaknesses identified above. Baseline security configurations help to ensure that organizations appropriately configure systems according to established technical and security policies and procedures, as well as the Medical Center Security Standard. The Medical Center Security Standard, section CM-2, requires documented baselines for information system components. Without an established baseline configuration, the Medical Center increases the risk that they will not implement minimum-security requirements to protect sensitive data they transmit on the wireless network.

The Medical Center should review, analyze, and document the settings and configurations to manage their WLAN. The Medical Center should also ensure that the wireless configurations and setting for all devices supporting the WLAN meet the requirements in the Medical Center Security Standard and align with best practices, such as the CIS Benchmark. Finally, the Medical Center should apply the settings and configurations to protect the confidentiality, integrity, and availability of mission critical and sensitive data.

Improve Patient Accounting, Billing, and Management System Segregation of Duties

Applicable to: Medical Center
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The Medical Center is not properly monitoring and analyzing security templates for its patient accounting, billing, and management system to ensure roles assigned are reasonable and align with the principle of least privilege. In fiscal year 2018, the University of Virginia Audit Department issued a segregation of duties audit report, which focused on access to the Medical Center's newly implemented patient accounting, billing, and management system. The primary issues noted by the Audit Department include insufficient consideration or analysis of potential segregation of duties conflicts when changing user access templates, along with a lack of documented approval when making changes to templates.

User access templates include various classes, and each class contains detailed security points. These security points are the key to assigning and restricting access in the patient accounting, billing, and management system. The Medical Center Security Standard, section AC-5 Separation of Duties, requires that the organization separate duties of individuals, document separation of duties of individuals, and define information system access authorizations to support separation of duties. With no documented analysis over sensitive security points in the patient accounting, billing, and management system coupled with a lack of documentation showing various changes that have been made to security templates since implementation, the Medical Center has limited assurance that access assigned complies with the principle of least privilege. Improper access to the patient accounting, billing, and management system increases the risk of improper activity within the system, which could subsequently affect the Medical Center's financial statements.

The Medical Center should follow recommendations made by the University of Virginia Audit Department related to segregation of duties in the patient accounting, billing, and management system.

By identifying and documenting sensitive security points, the Medical Center will be able to better analyze security templates to monitor for improper segregation of duties within the system.

Improve Bank Reconciliation Policies and Procedures
Applicable to: Medical Center
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

The Medical Center should refine its bank reconciliation process and related cash procedures to address the following items noted during the fiscal year 2018 audit, including:

- The Medical Center does not have updated written procedures for current Medical Center processes related to bank reconciliations. Currently, there is a lack of documentation related to who should perform the various procedures, how often to perform the applicable procedures, and who should review the completed reconciliations. For all three reconciliations tested during the fiscal year 2018 audit (August 2017, November 2017, and June 2018), there was no evidence as to when the reconciliation was prepared, who prepared the reconciliation, and who reviewed the reconciliation. Proper written procedures help minimize process interruption in the event of an unexpected departure of a key employee.

- The Medical Center currently reconciles transactions on a daily basis, and a summary log is prepared monthly to show monthly bank activity. The current process is adequate to identify daily reconciling items; however, the Medical Center does not have a month-end process that shows a cumulative reconciliation between the general ledger and the bank statements. With no bank to general ledger reconciliation, there is no way to ensure that the Medical Center is properly addressing past reconciling items, and no way to show that the general ledger balances reconcile to the Medical Center's bank accounts. For the reconciliations reviewed, there was no evidence in the month-end log that the Medical Center properly addressed reconciling items identified during the daily reconciliation process.

The University of Virginia Medical Center should develop policies and procedures to properly reflect current bank reconciliation processes in accordance with best practices. Additionally, developing a cumulative reconciliation will provide additional evidence that general ledger cash accounts reconcile to Medical Center bank accounts and that the Medical Center identifies and addresses reconciling items in a timely manner.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 27, 2018

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
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, 2018, 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 27, 2018. Our report includes a reference to other auditors. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of the University, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion 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 Security Awareness Training Program," "Improve IT Risk Management Process and Documentation," "Improve Oversight of Third-Party Service Providers (Academic and Medical Center Divisions)," "Improve Database Security," "Improve Revenue Recognition for Non-reimbursement Grants," "Improve Notification Process for Federal Direct Loan Awards to Students," "Promptly Return Title IV Funds," "Improve Reporting to the National Student Loan Data System," "Improve Wireless Local Area Network Security," "Improve Patient Accounting, Billing, and Management System Segregation of Duties," and "Improve Bank Reconciliation Policies and Procedures," which are described in the sections titled "Status of Prior Year Findings and Recommendations" and "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 of Virginia'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 Security Awareness Training Program," "Improve IT Risk Management Process and Documentation," "Improve Oversight of Third-Party Service Providers (Academic and Medical Center Divisions)," "Improve Database Security," "Improve Notification Process for Federal Direct Loan Awards to Students," "Promptly Return Title IV Funds," "Improve Reporting to the National Student Loan Data System," "Improve Wireless Local Area Network Security," and "Improve Patient Accounting, Billing, and Management System Segregation of Duties."

The University's Response to Findings

We discussed this report with management at an exit conference held on November 26, 2018. The University's response to the findings identified in our audit is described in the accompanying section titled "University Response." The University's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings

The University has not completed corrective action with respect to the previously reported findings included in the section entitled "Status of Prior Year Findings and Recommendations." The University of Virginia 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/vks

Improve Oversight of Third-Party Service Providers
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

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

Responsible for Corrective Action: Jason Belford, Chief Information Security Officer

Anticipated Completion Date: March 31, 2019

Corrective Action to be taken by the University Management:
As mentioned in the APA's finding, the University has conducted a review of some SOC reports, albeit on an informal basis. The University will determine the resources needed to create and maintain a formal process to request the high priority SOC reports from each vendor and review them on an annual basis. By the end of March 2019, ITS, Information Security, Finance, and General Counsel will create a plan to move forward to review high priority SOC reports, annually, and will ensure that this plan is executed and properly documented.

Improve Database Security
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

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

Responsible for Corrective Action: Teresa Wimmer, AVP for Enterprise Applications

Anticipated Completion Date: March 31, 2019

Corrective Action to be taken by the University Management:
The University believes the risk related to the database security to be minimal, given the restricted access and the length of service of the employees who have access, and given the large customer base that has followed the vendor's guidelines for database settings to support their applications. That said, the University will develop a database hardening process and implement it by the end of March 2019.

As we develop this process, we will evaluate each of the measures listed in the APA's finding and implement those that do not cause interference with the operational capabilities of our systems.

Improve Revenue Recognition for Non-reimbursement Grants
Applicable to: Academic Division
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

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

Responsible for Corrective Action: Thomas Schneeberger, Director of Financial Reporting

Anticipated Completion Date: June 30, 2019

Corrective Action to be taken by the University Management:
Financial Reporting has identified and formalized a process to properly recognize certain grant revenue on an annual basis going forward. The overstatement of unearned revenue was discovered by Financial Reporting staff, brought to the attention of the APA, and resolved by posting the necessary adjustments before the FY2018 financial reporting deadline. In addition, Financial Reporting will evaluate the most common and significant auto-accounting rules on at least on a yearly basis to ensure that the rules align with the environment and current activity of the University.

Improve Notification Process for Federal Direct Loan Awards to Students
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

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

Responsible for Corrective Action: Steve Kimata, AVP for Student Financial Services

Anticipated Completion Date: June 30, 2019

Corrective Action to be taken by the University Management:
The University immediately corrected the underlying systems to ensure that all required disclosures are sent to students on a timely basis. SFS will closely monitor the notification process and system on a regular basis going forward to ensure continued compliance.

Promptly Return Title IV Funds
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

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

Responsible for Corrective Action: Steve Kimata, AVP for Student Financial Services

Anticipated Completion Date: June 30, 2019

Corrective Action to be taken by the University Management:
The University has promptly implemented improvements to existing processes that ensures accurate monitoring and the timely return of Title IV funds, including additional controls that alert management to the transactions and impending deadlines.

Improve Reporting to the National Student Loan Data System
Applicable to: Academic Division
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Management Response:
The University of Virginia's understanding of the federal regulations with regards to the effective enrollment change date and the date of determination differs from the APA. Based on the University's interpretation of both the Code of Federal Regulations and the NSLDS Reporting Guide, we feel that we are in compliance with NSLDS requirements. The University has consulted with the National Student Clearinghouse (NSC), the organization that delivers financial aid student enrollment certifications to the NSLDS for UVA and most colleges in regards to the NSLDS requirements and these specific students.

Responsible for Corrective Action: Steve Kimata, AVP for Student Financial Services

Anticipated Completion Date: June 30, 2019

The University interprets the Code of Federal Regulations in conjunction with the NSLDS Reporting Guide which states that the "Department defers to a school's policy regarding the establishment of effective dates" (Section 4.4.2 of the Guide). The University acknowledges that the University's effective enrollment status date for a student's withdrawal is set in a manner to provide the student with ability to reconsider his/her initial consideration of withdrawal and receive counseling; only after

that does the University set the effective enrollment change date and report changes to the NSLDS. When the University follows the NSLDS Reporting Guide on the establishment of an effective date based on the University's withdrawal policy, the University's reporting to the NSLDS is completed on a timely basis. The University is willing to work in concert with the APA to request additional guidance regarding the establishment of an enrollment status change from the Department of Education and to clarify reporting procedures with the National Student Clearinghouse.

Improve Wireless Local Area Network Security
Applicable to: Medical Center
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

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

Responsible for Corrective Action: Erin Trost

Anticipated Completion Date: June 30, 2019

Corrective Action to be taken by the University Management:
The UVA Medical Center is currently working on a project to redefine patch cycles for IT related infrastructure. As part of this project, teams will re-assess patch management related standards and develop patch cycles based on best in practice standards. The new patch management standard will include an exception process for patches that cannot be applied within the standard patch management cycle. These exceptions will be reviewed by executive leadership and sign off will be required.

Improve Patient Accounting and Billing System Segregation of Duties
Applicable to: Medical Center
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

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

Responsible for Corrective Action: Erin Trost

Anticipated Completion Date: June 30, 2019

Corrective Action to be taken by the University Management:
The UVA Medical Center's Revenue Cycle team, in partnership with UVA Internal Audit, is reviewing and defining roles which may constitute potential segregation of duties issues. In addition, a governance group (incl. Revenue Cycle and Patient Billing Application teams) has been formed and is following the action plan established by UVA Internal Audit.

Improve Bank Reconciliation Policies and Procedures
Applicable to: Medical Center
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

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

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

Anticipated Completion Date: June 30, 2019

Corrective Action to be taken by the University Management:
The UVA Medical Center has created a detailed work assignment matrix to include workflow processes as well as related desk procedures by individual. In addition, the Medical Center will have a fully implemented bank reconciliation process for FY19, including a more defined process to resolve and clear reconciling items. The bank reconciliation will include a list of reconciling items and a reconciliation of the net change between bank cash and the cash balance in the General Ledger.

UNIVERSITY OF VIRGINIA

As of June 30, 2018

BOARD OF VISITORS

Frank M. Conner, III
Rector

James B. Murray, Jr.
Vice Rector

Robert M. Blue
Mark T. Bowles
L.D. Britt
Whittington W. Clement
Elizabeth M. Cranwell
Thomas A. DePasquale
Barbara J. Fried
John A. Griffin
Robert D. Hardie
Maurice A. Jones
Babur B. Lateef
Tammy S. Murphy
C. Evans Poston, Jr.
James V. Reyes
Jeffrey C. Walker

Brendan T. Nigro
Student Representative

Margaret F. Riley
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