# UNIVERSITY OF VIRGINIA

## REPORT ON AUDIT
## FOR THE YEAR ENDED
## JUNE 30,2021

Auditor of Public Accounts
Staci A. Henshaw, 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, 2021, and issued our report thereon, dated December 3, 2021. Our report is included in the University's Financial Report, 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 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 programs of the Student Financial Aid Cluster, Education Stabilization Fund, and Provider Relief Fund for the Commonwealth's Single Audit as described in the U.S. Office of Management and Budget Compliance Supplement; 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 Controls over User Access to the Payroll and Human Resources System**
**Applicable to:** All Divisions
**Responsible Department:** University Human Resources Office
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency
**Repeat:** Yes (partial, first issued for fiscal year 2019)

The University of Virginia (University) has not developed a resource to adequately evaluate conflicting business processes and their respective user access roles in their Payroll and Human Resources System (System). Without this resource there is an increased risk that University employees are assigned roles in the System that create segregation of duty conflicts, resulting in a heightened reliance on detective controls to reduce the risk of fraudulent transactions and errors in financial reporting. The University did implement controls to address significant deficiencies outlined in a report issued by the University's Internal Audit Department (Internal Audit) in May 2020 that is referenced in our prior year report, and these controls do reduce the risk of improper System access. However, the lack of a resource to evaluate potential segregation of duty conflicts make the provisioning and access review controls implemented to address Internal Audit's findings less effective. The University did not develop a resource to identify potential conflicts due to personnel resources being prioritized to address deficiencies identified by Internal Audit.

As outlined in the University's policy FIN-021: Internal Control, individuals responsible for administering University funds and resources must grant or delegate financial authority carefully, with consideration for proper segregation of duties. The University's adopted information security standard, ISO 27002, Section 9.2.2 states, "the provisioning process for assigning or revoking access rights granted to user IDs should include verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties."

The University should allocate personnel to develop a resource that details conflicting business processes and their respective roles for use in establishing and monitoring future access to the System.

**Improve Processes over Employment Eligibility Verification**
**Applicable to:** All Divisions
**Responsible Department:** University Human Resources Office
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency
**Repeat:** Yes (partial, first issued for fiscal year 2020)

The University Human Resources department (Human Resources) continues to improve the University's process to ensure compliance with Employment Eligibility Verification (I-9) Form completion. Human Resources implemented procedures effective August 2020 to detect non-compliance more effectively and reduce delays in Form I-9 completion. However, we found that Human

Resources did not comply with guidelines issued by the U.S. Citizenship and Immigration Services of the U.S. Department of Homeland Security for six employee I-9 forms out of a sample of 22 randomly selected employees (27%). The applicable compliance criteria resulting in exceptions are as follows:

- four out of 22 employees selected (18%) did not complete and sign Section 1 of the Form I-9 by the first day of employment;

- the Human Resources Officer did not complete Section 2 within three business days after the first day of employment for four out of 22 (18%) employees; and

- Human Resources did not create a case in E-Verify within three business days for four out of 22 (18%) employees.

The Immigration Reform and Control Act of 1986 requires employers to verify employment eligibility and identify for all employees hired after November 6, 1986, by using Form I-9. U.S. Citizenship and Immigration Services sets forth federal requirements for completing the Form I-9 in the Handbook for Employers M-274 (the Handbook). Chapter 3 of the Handbook requires the employee to complete and sign Section 1 of the Form I-9 by the first date of employment. Chapter 4 of the Handbook requires the employer to complete Section 2 of Form I-9 within three business days of the first date employment. Chapter 2.2 of the E-Verify User Manual requires employees to create a case in E-Verify no later than the third business day after the employee starts work. Noncompliance with federal regulations related to employment verification could result in civil and/or criminal penalties and debarment from government contracts.

The decentralized nature of the hiring and on-boarding process is the primary cause of noncompliance. Each applicable school is responsible for hiring and subsequently recording and activating each new hire in the System. Employees cannot complete a Form I-9 until they are active in the System, and delays in this process create little to no time for an employee to complete their Form I-9 on the first day of employment. Monitoring controls implemented by Human Resources in August 2020 are effective to identify noncompliance after it occurs; however, monitoring controls are not a substitute for having an effective process to prevent noncompliance. Human Resources should develop procedures to ensure new hires are timely entered into the System by each decentralized school responsible for hiring and to ensure compliance with employee eligibility requirements.

## INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

**Complete Annual Review Over User Access to University Information Systems**
**Applicable to:** Academic Division
**Responsible Department:** Information Technology Services
**Type:** Internal Control
**Severity:** Significant Deficiency
**Repeat:** No

The University of Virginia Academic Division (Academic Division) did not perform an adequate annual review and re-verification of users with access to two Academic Division systems containing sensitive data. We found that the Academic Division Registrar conducted a review of student information system users within their department; however, a review over all other student information system users throughout the Academic Division was not performed. We also found that the Academic Division senior financial controls coordinator conducted a high-level summary review of users with access to the Academic Division's accounting and financial reporting system; however, each user's access was not individually reviewed and re-verified as being appropriate by a manager or data access approver familiar with the user's job responsibilities.

As outlined in the Academic Division's policy Sec-037: Networks, Systems, and Facilities Access & Revocation and the Issue & Return of Tangible Personal Property, "User access to all University systems of record and any system used to process, store, transfer, or access highly sensitive data must be re-verified annually." The lack of a sufficient annual access review process increases the risk of improper or unnecessary access to sensitive systems, which could result in a breach in data security. This finding resulted from the Academic Division not designating specific personnel and/or departments to perform the annual access reviews.

The Academic Division should consider including designated personnel and/or departments who are responsible for the University's student information system and accounting and financial reporting system annual access reviews within the University's policy Sec-037, which will help ensure that annual access reviews over these systems are being completed.

**Implement Information Security Program Requirements for the Gramm-Leach-Bliley Act**
**Applicable to:** Academic Division
**Responsible Department:** Student Financial Services Office and Information Technology Services
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency
**Repeat:** No

The Academic Division does not consider certain required elements of the Gramm-Leach-Bliley Act (GLBA) within the Academic Division risk assessments of systems containing nonpublic customer information. The Academic Division completed a risk assessment for two systems that contain nonpublic customer information. However, the risk assessments do not include all required elements of the GLBA.

Additionally, the Academic Division did not assess the risk for all systems that contain nonpublic customer information.

Institutions of higher education, because of their engagement in financial assistance programs, are considered financial institutions that must comply with Public Law 406-12, also known as the GLBA. Related regulations at 16 C.F.R. 314.4 require organizations to develop, implement, and maintain the information security program to safeguard nonpublic customer information and complete a risk assessment that includes consideration of risks and mitigating controls in each relevant area of operations. The regulations require a risk assessment that considers the following elements:

- employee training and management;
- information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and
- detecting, preventing, and responding to attacks, intrusions, or other system failures.

Without implementing cybersecurity requirements of the GLBA for each system containing nonpublic customer information, the Academic Division may not be able to ensure the security and confidentiality of customer information. Additionally, the Academic Division may not protect against anticipated threats or hazards to the security or integrity of such information and protect against unauthorized access to or use of nonpublic customer information that could result in substantial harm or inconvenience to any customer.

The Academic Division did not perform a risk assessment process from a university-wide perspective as it was unaware of the requirements of the GLBA and assumed that their system risk assessments would meet the requirements. This caused the Academic Division to not consider certain risks that may impact its information technology (IT) environment and safeguards that are either in place or that need to be implemented to mitigate those risks, respectively.

The Academic Division should include all elements in its risk assessment process as required by GLBA and document those risks that may impact the IT environment. As part of the risk assessment process, the Academic Division should identify controls and safeguards that are either in place or need to be implemented that mitigate the risks identified in the risk assessment. If there are controls that need to be implemented, the Academic Division should develop and implement a corrective action plan that includes controls to mitigate the risks. This process will assist the Academic Division in evaluating its information security program and protecting the confidentiality, integrity, and availability of student information within its environment.

**Promptly Return Unclaimed Aid to Department of Education**
**Applicable to:** Academic Division
**Responsible Department:** Student Financial Services Office
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency
**Repeat:** No

The Academic Division Student Financial Services Office (Student Financial Services) personnel did not return unclaimed student financial aid funds to the U. S. Department of Education within the required timeframe. Specifically, at the time of audit, Student Financial Services Office personnel had not returned a total of $55,692. Academic Division management indicated the delays resulted from COVID-19 operational changes including but not limited to adapting to changes with the start dates of the fall and spring terms; adjusting housing and dining charges; prioritizing student relief by suspending collection activity; processing significantly increased volumes of student refunds; tracking and adjusting changes with the comprehensive fee and revised billing due dates; and transitioning of staff responsibilities.

In accordance with 34 C.F.R 668.164(l), if an institution attempts to disburse the funds by check and the check is not cashed, the institution must return the funds no later than 240 days after the date it issued that check or no later than 45 days after an electronic funds transfer is rejected. By not returning funds timely, the institution is subject to federal non-compliance and potential adverse actions that may affect the Academic Division's participation in Title IV aid programs.

In the event the Academic Division is unable to contact the federal aid recipient and the check remains uncashed, the Academic Division should ensure that unclaimed funds are returned to the Department of Education within the required timeframe.

**Properly Complete Exit Counseling for Direct Loan Borrowers**
**Applicable to:** Academic Division
**Responsible Department:** Student Financial Services Office
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency
**Repeat:** No

The Academic Division Student Financial Services did not confirm all federal Direct Loan borrowers that graduated or withdrew completed online exit counseling. Academic Division management indicated the delays resulted from COVID-19 operational changes including but not limited to adapting to changes with the start dates of the fall and spring terms; adjusting housing and dining charges; tracking and adjusting changes with the comprehensive fee and revised billing due dates; and a need to refine the process. From a review of 35 students, we identified the following deficiencies:

- for five borrowers (14%), Student Financial Services did not provide the required exit counseling materials;

- for three borrowers (9%), Student Financial Services did not provide the required exit counseling materials timely; and

- for one borrower (3%), Student Financial Services did not provide the required exit counseling materials to an email address that is not associated with the school.

In accordance with 34 C.F.R. 685.304(b)(3), if a student borrower withdraws from a school without the school's prior knowledge or fails to complete the exit counseling as required, exit counseling must, within 30 days after the school learns that the student borrower has withdrawn from the school or failed to complete the exit counseling as required, be provided either through interactive means, by mailing written counseling materials to the student borrower at the student borrower's last known address, or by sending written counseling materials to an email address provided by the student borrower that is not an email address associated with the school sending the counseling materials. By not performing this function, students may not receive the relevant information related to repayment of their student loans.

Student Financial Services should review their policies and procedures for sending exit counseling materials to students and implement corrective action to ensure all applicable students are properly notified of exit counseling requirements timely.

**Continue to Improve Controls and Compliance with Student Financial Aid Requirements**

**Applicable to:** UVA College at Wise

**Responsible Department:** UVA College at Wise Financial Aid Office

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**Repeat:** No (issued in separate report dated September 7, 2021)

**Prior Title:** Improve Reporting to the Common Origination and Disbursement System; Improve Federal Direct Loan Borrower Notification Process; Report Student Status Changes Accurately and Timely to the National Student Loan Data System; Perform Accurate Title IV Calculations; Promptly Return Unearned Title IV Aid to Department of Education; Ensure an Accurate FISAP is Submitted to Department of Education; Perform Federal Direct Loan Reconciliations Timely; Enhance Notification for Federal Direct Loan Borrowers that have not Completed Exit Counseling; Improve Direct Loan Quality Assurance Program; and Strengthen Compliance with the Gramm-Leach Bliley Act

The University of Virginia's College at Wise (Wise) should continue to address our findings related to its management of federal student financial assistance issued under a separate report dated September 7, 2021. Our audit covered the fiscal year ended June 30, 2020, and identified the following internal control findings and instances of noncompliance.

- Wise did not report disbursements timely or accurately to the federal Common Origination and Disbursement System.

- Wise sent notifications to federal Direct Loan borrowers; however, the notifications did not include all required elements prescribed by the Code of Federal Regulations (C.F.R.).

- Wise did not report enrollment data to the National Student Loan Data System accurately and/or timely.

- Wise did not perform accurate return of Title IV calculations.

- Wise's financial aid office did not complete return of Title IV calculations for summer 2019, fall 2019, and spring 2020 until June 2021. The delay in completing the calculations resulted in unearned aid for some students withdrawing during summer 2019, fall 2019, and spring 2020 not being returned within 45 days of the Wise's determination that each student had withdrawn.

- Wise did not submit an accurate Fiscal Operations Report and Application to Participate (FISAP).

- Wise was unable to provide sufficient documentation showing that all required federal Direct Loan reconciliations have been completed monthly as required.

- Wise did not consistently send notifications to federal Direct Loan borrowers regarding the requirement to complete exit counseling.

- Wise did not have a documented federal Direct Loan quality assurance program that is accessible and available for review.

- Wise was not able to provide audit evidence to indicate full compliance with the Gramm-Leach-Bliley Act (GLBA).

In accordance with 2 C.F.R. 200.303, non-federal entities must establish and maintain effective internal control over federal awards that provides reasonable assurance that the non-federal entity is managing federal awards in compliance with federal statutes, regulations, and terms and condition of the federal award. These findings resulted from significant turnover within the Wise's financial aid office and lack of management oversight. Due to the timing of the issuance of our report, Wise's management did not have adequate time to complete corrective action prior to June 30, 2021. Therefore, we plan to follow up on corrective action in a subsequent audit. Wise's management should continue to monitor the implementation of the corrective action plans to resolve these findings.

**Allocate Additional Resources for Financial Statement Preparation**

**Applicable to:** Medical Center
**Responsible Department:** Controller's Office
**Type:** Internal Control
**Severity:** Significant Deficiency
**Repeat:** No

The University of Virginia Medical Center (Medical Center) did not fully adhere to the Governmental Accounting Standards Board (GASB) financial statement presentation requirements for a majority equity interest in a legally separate entity meeting the definition of a component unit. While appropriate adjustments have been made to the financial statements to ensure fair presentation of the Medical Center's financial statements, the Medical Center did not complete required entries, associated adjustments, and note disclosures in a timely manner which delayed completion of audit field work past the anticipated audit completion date. GASB prescribes generally accepted accounting principles (GAAP) for governmental entities. Per GASB Codification §1200.101, "GAAP are uniform minimum standards of and guidelines to financial accounting and reporting. Adherence to GAAP assures that financial reports of all state and local governments contain the same types of financial statements and disclosures." Further, in GASB Concept Statement 1, Objectives of Financial Reporting, "nothing material should be omitted from the information necessary to faithfully represent the underlying events and conditions, nor should anything be included that would cause the information to be misleading." Failure to present financial activity in accordance with GAAP may impact stakeholders' ability to rely on the Medical Center's financial statements to make informed decisions.

The Medical Center's financial statements are complex and unique. The Medical Center is a governmental hospital that is also a division of the University. The Medical Center prepares individual financial statements, which include the Medical Center and its subsidiaries, and these financial statements serve as a starting point for Medical Center financial information included in the consolidated financial statements of the University. GASB's application of GAAP does not, in all cases, prescribe specific treatment for an entity like the Medical Center. Further, governmental accounting standards are constantly evolving and have become more complex in recent years. The complexity and lack of comparable governmental reporting entities makes it difficult for staff who function in a split general accounting and financial statement reporting capacity to keep up to date on current accounting and financial reporting standards that impact financial statement presentation and disclosure. The Medical Center relies on its Controller for both general internal accounting and external financial statement preparation functions.

Due to the complexity associated with governmental hospital and government departmental financial statements, the Medical Center should develop a plan to engage additional resources to assist with preparation of year-end financial statements to ensure adherence to the presentation requirements prescribed by GASB. Employing additional resources will also help to improve the timeliness of financial statement reporting by lessening the daily, monthly, and yearly burden vested in a single position.

**Improve Accuracy of Provider Relief Fund Reporting**
**Applicable to:** Medical Center
**Responsible Department:** Third Party Reimbursement
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency
**Repeat:** No

The Medical Center reported expenses reimbursed via other federal sources as Provider Relief Fund (PRF) expenses in its required Health and Human Services Health Resources and Services Administrator (HRSA) report. HRSA's PRF Reporting User Guide (the Guide), Section 4.10, states that the reporting entity is to use the Other PRF Expenses section of the report to submit quarterly expenses reimbursed with "Other PRF Payments." The Guide defines "Other PRF Payments" as "all General Distribution payments and Targeted Distribution payments, except for those payments categorized as Nursing Home Infection Control payments." The Medical Center received general distribution payments due to its status as a recognized Medicare fee-for-service provider. In addition, the Medical Center overstated the lost revenues it reported in the Lost Revenues section of its HRSA PRF report by $3.5 million due to the inclusion of a legally separate component unit that filed a separate HRSA PRF report for its use of PRF funds.

Per Medical Center management, the Medical Center intended to apply its PRF general distribution payments to lost revenues, as allowed under the terms and conditions of the PRF. Per Section 4.13 of the Guide, the calculation of lost revenues "will be applied to the balance of the Other PRF payments (after reported expenses are deducted) to determine the total dollar amount of PRF payments expended for the Payment Received Period." A misunderstanding of what was to be reported in the Other PRF Expenses section of the HRSA PRF report resulted in improper inclusion of expenses reimbursed by non-PRF sources. Additionally, frequently asked questions published by HRSA provide guidance stating parent entities may report on a subsidiary's general distribution payments regardless of which organization received the general distribution payment. However, as the Medical Center did not report on its subsidiary's general distribution payments as part of the Medical Center's HRSA PRF report, it should have excluded associated lost revenues for the subsidiary to allow for appropriate separate reporting to HRSA. Inclusion of lost revenues associated with the Medical Center's subsidiary was due to an oversight during the preparation of the report and a lack of secondary review by Medical Center personnel independent of the preparation of the report. As a result of improperly reporting expenses in the Other PRF Expenses section and overstating lost revenues in the HRSA PRF report, the Medical Center supplied HRSA with incorrect information regarding its use of PRF receipts.

The Medical Center should seek to clarify any uncertainty regarding PRF reporting requirements by directly contacting HRSA and should consider implementing a secondary review process to ensure proper reporting in accordance with the Guide. Additionally, the Medical Center should revise the information reported in steps nine and twelve of its HRSA report in its next reporting submission. Ensuring the accuracy of information will help to improve HRSA's ability to make appropriate decisions based on data reported.

**Improve Firewall Patch Management**
**Applicable to:** Medical Center
**Responsible Department:** Health System Technology Services
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency
**Repeat:** No

The Medical Center does not secure its enterprise firewall in accordance with its policies and its adopted security standard, the National Institute of Standards and Technology Standard, 800-53 (NIST Standard).

We communicated the internal control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The NIST Standard requires the implementation of certain controls to reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information. By not meeting the minimum requirements in the NIST Standard, the Medical Center is not reducing unnecessary risk that may impact the confidentiality, integrity, and availability of sensitive and mission critical data.

The Medical Center should implement the security controls discussed in the communication marked FOIAE in accordance with the NIST Standard.

**Improve Security Awareness Training**
**Applicable to:** Medical Center
**Responsible Department:** Health System Technology Services
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency
**Repeat:** No

The Medical Center is not meeting certain security awareness training (SAT) requirements in the NIST Standard. The Medical Center does not ensure all users complete SAT and the Medical Center does not provide role-based training to users with specific information security roles and responsibilities. An established SAT program is essential to protecting Medical Center IT systems and data by ensuring that employees understand their roles and responsibilities in securing sensitive information. Specifically, our review of the Medical Center's SAT program identified the following weaknesses:

- The Medical Center does not enforce compliance with security awareness training requirements, which resulted in 591 users (6.67%) not completing the assigned SAT. The Medical Center's Security Awareness Policy requires that users complete initial and annual refresher training, that users not completing the training will have access suspended, and that the user's supervisor must notify Health Information Technology to suspend access due to noncompliance. However, the Medical Center is not currently suspending user access when the user does not complete required training. Additionally, the NIST Standard requires that all computer users complete SAT initially upon employment, after significant changes in

the environment, and at organizationally defined intervals thereafter (NIST Standard section: AT-2 Security Awareness). Without ensuring that all users complete SAT annually, the Medical Center increases the risk that users will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

- The Medical Center does not require or provide role-based training to users with designated information security roles, such as system owners, data owners, system administrators, and security personnel. The Medical Center's Security Awareness Policy includes requirements for employees to complete at-hire security training and annual refresher training; however, the policy does not include a requirement for role-based training for users with designated information security roles. The NIST Standard requires role-based training initially, when required by information system changes, and at organizationally defined intervals thereafter for personnel with assigned security roles and responsibilities (NIST Standard section: AT-1 Security Awareness and Training Policy and Procedures; NIST Standard section: AT-3 Role-Based Security Training). Insufficient role-based training increases the risk that users will be unaware or lack pertinent skills and knowledge to perform their security related functions, increasing the risk to sensitive data.

Although supervisors send email notifications of noncompliance to employees who do not take required SAT, the Medical Center is unable to ensure SAT completion, as required by the Medical Center's policy, without using the enforcement measure to disable user access. Human Resources and supervisors are tasked with informing the Health Information Technology team of users that have not completed SAT. However, lack of communication between Human Resources and supervisors resulted in Health Information Technology not receiving a list of non-compliant users for access termination. Additionally, the Medical Center has not prioritized providing role-based training for users with designated information security roles but is beginning the process of creating modules for personnel with assigned security roles and responsibilities.

Health Information Technology and Human Resources should develop a formal process to notify Health Information Technology to suspend access due to noncompliance to ensure that all users complete SAT before accessing computer resources and on an annual basis thereafter. Additionally, the Medical Center should develop a procedure, then create and implement the necessary modules to provide role-based training to users with designated security roles. Improving the SAT program will help protect the Medical Center from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data.

Commonwealth of Virginia

*Auditor of Public Accounts*

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 3, 2021

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Kenneth R. Plum
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, aggregate discretely presented component units, and remaining fund information of the **University of Virginia** as of and for the year ended June 30, 2021, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated December 3, 2021. 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 (internal control) as a basis for designing 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. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

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 was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control 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 that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve Controls over User Access to the Payroll and Human Resources System," "Improve Processes over Employment Eligibility Verification," "Complete Annual Review Over User Access to University Information Systems," "Implement Information Security Program Requirements for the Gramm-Leach Bliley Act," "Promptly Return Unclaimed Aid to Department of Education," "Properly Complete Exit Counseling for Direct Loan Borrowers," "Continue to Improve Controls and Compliance with Student Financial Aid Requirements," "Allocate Additional Resources for Financial Statement Preparation," "Improve Accuracy of Provider Relief Fund Reporting," "Improve Firewall Patch Management," and "Improve Security Awareness Training," 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'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 financial statements. 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 titled "Improve Controls over User Access to the Payroll and Human Resources System," "Improve Processes over Employment Eligibility Verification," "Implement Information Security Program Requirements for the Gramm-Leach Bliley Act," "Promptly Return Unclaimed Aid to Department of Education," "Properly Complete Exit Counseling for Direct Loan Borrowers," "Continue to Improve Controls and Compliance with Student Financial Aid Requirements," "Improve Accuracy of Provider Relief Fund Reporting," "Improve Firewall Patch Management," and "Improve Security Awareness Training."

## The University's Response to Findings and Recommendations

We discussed this report with management at an exit conference held on November 29, 2021. 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 "Improve Controls over User Access to the Payroll and Human Resources System," and "Improve Processes over Employment Eligibility Verification." 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 Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

DLR/clj

UNIVERSITY of VIRGINIA | UVAFinance

December 3, 2021

Ms. Staci Henshaw
Commonwealth of Virginia Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw,

We have reviewed the audit findings and recommendations resulting from the fiscal year 2021 audit related to the University of Virginia (UVA) Academic Division (University) and Medical Center. Below are management's responses to those findings.

**ACADEMIC DIVISION**

**Properly Complete Exit Counseling for Direct Loan Borrowers**
**Management Response:** The UVA Academic Division concurs with the APA's finding.
**Responsible for Corrective Action:** Steve Kimata, Assistant VP Student Financial Services
**Anticipated Completion Date:** December 2021

After the oversight was discovered, Student Financial Services (SFS) sent exit counseling information to the five (5) student borrowers from the test sample and all other students we identified who borrowed in 2021 who had not previously received exit counseling information.

SFS has updated our controls and procedures for monitoring and initiating exit counseling. These updates include ensuring that all students who need exit counseling are properly identified, importing NSLDS loan history into the Student Information System, monitoring COD for completion of exit counseling, and sending exit counseling information to student borrowers' non-University email address (when available), all within the required timeframe.

**Promptly Return Unclaimed Aid to Department of Education**
**Management Response:** The UVA Academic Division concurs with the APA's finding.
**Responsible for Corrective Action:** Steve Kimata, Assistant VP Student Financial Services
**Anticipated Completion Date:** December 2021
Student Financial Services (SFS) has implemented additional controls for monitoring unclaimed checks containing Title IV funds. These enhanced procedures include: assigning additional staff to review and execute monthly reporting; utilizing new methods to contact students or parents along with

increasing the frequency of the outreach; and returning unclaimed Title IV funds to the Department of Education within the prescribed timeframes. These enhanced procedures would have promptly returned to the Department of Education the $55,692 of unclaimed student financial aid funds that SFS personnel did not return to the Department of Education within the required timeframe, which represents 0.3% of all Title IV monies refunded by UVA.

**Improve Processes over Employment Eligibility Verification**
**Management Response:** UVA concurs with the finding with additional clarification provided.
**Responsible for Corrective Action:** Adam Weikel, Assistant Vice President for HR Service; Jennifer Weaver, Talent Support Manager; Julie Bird, Sr. Director of Continuous Improvement HR
**Anticipated Completion Date:** June 2022

The University of Virginia has reviewed the 6 instances of noncompliance noted in the APA's sample and notes additional factors that should be considered in evaluating the management point:

In one situation there was a technical issue with the employee's record in the HR system in which hires are processed and I-9s are completed. This did not allow for the new employee or UVA HR to complete an I-9 timely. Due to COVID restrictions at the time (August 2020), we were unable to meet with the employee in person to complete the I-9 within 3 business days which would have eliminated the system issue and cause for incompliance. The remote option was our only recourse and with a system issue related to this hire's record (which required technical intervention), it was impossible to complete the I-9 timely. This circumstance is not a systemic issue, but an exception scenario, which would be approved by E-Verify upon audit.

In the other 3 situations where Part I was not completed by day 1 of hire, all three were hired retroactively in the system. Because FLSA requires employees to be paid for all hours worked, the hires had to be entered to ensure the employees were paid correctly. Since the hires were retro-dated, the employees were not able to complete Part I of I-9 timely. In all three scenarios, the hires were completed by the Department of the hires and not directly by UVA HR.

In 2 of the remaining 3 scenarios where Part II of the I-9 was not completed timely by UVA HR, Part I was reviewed by UVA HR and we noted incorrect information. Part I was sent back to the employee to correct the information and re-submit it to UVA HR in the HR system. If UVA HR had processed Part II at the time it was received, both I-9s would have been in compliance. However, if approved, they would have also resulted in a TNC with E-Verify creating more work for both the employee and UVA HR to resolve. It is UVA HR's responsibility to ensure the I-9 is completed accurately before submitting it to E-Verify.

As noted in last year's audit finding, UVA HR created audit reports to help capture late hires by the

*UVAFinance is the valued and trusted financial partner that the University community turns to first.*
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | F 434.982.2315 | vpfinance@virginia.edu

schools/departments across the organization. In review of this year's data as compared to last year's, there has been a significant improvement in the number of days late on any occurrences and a decrease in percentage of I-9s out of compliance for Part I (2020 – 28%, 2021- 18%) and Part II (2020 – 38%; 2021 – 18%).

UVA HR has created a daily audit report in our Payroll and Human Resources System that uses live data for our I-9 tracking list. This will continue to allow us to begin communication as soon as the hire is completed in Workday and will save time in running weekly/monthly audit reports.

We believe all possible HR efforts are complete and we now need to engage with stakeholders in order to make further improvements. We recognize that the remaining improvement efforts reside within schools and units. As a result, we will organize an improvement initiative over the next year with a focus on schools and units, potentially including a communications campaign and engagement with the Provost Office, Associate Deans, and other school/unit leadership.

**Complete Annual Review Over User Access to University Information Systems**
**Management Response:** UVA concurs with the APA's finding.
**Responsible for Corrective Action:** Augie Maurelli, AVP for Financial Operation; Teresa Wimmer, AVP for Enterprise Applications
**Anticipated Completion Date:** June 2022

The University agrees with the APA's finding, that University policy SEC-037: Networks, Systems, and Facilities Access & Revocation and the Issue & Return of Tangible Personal Property, 8. Annual Audit and Review, does not identify ownership of the annual audit and review, nor does it assign clear responsibilities for performance of the review. The University also agrees with the APA's recommendation, to include designated personnel and/or departments who are responsible for conducting the annual access reviews of University systems, within University policy SEC-037. Compliance and policy representation from multiple areas, including UVA Finance, Student Financial Services, University HR, and ITS, will collaborate on reviewing and updating this policy.

Additionally, the related policy referenced in this section, IRM-003: Data Protection of University Information, Definitions in Terms of Statement, defines the role of Data Access Approvers as "officials who have responsibility for confirming that requests for access correctly map to what the data users need in the way of access to the specific components of a given application required to perform job duties, and for which they have appropriate training." This role is currently set up within the user access request workflow.
The University is undergoing significant change to its finance system, including a completely new set of user roles requiring definition, and changes to requesting access. Retirement of the tool, which has been used for system access requests, began prior to fiscal year end, and is being done in stages. The

*UVAFinance is the valued and trusted financial partner that the University community turns to first.*
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | F 434.982.2315 | vpfinance@virginia.edu

University is evaluating solutions to improve the process for user access requests, and also address the unique needs of each system (student information, finance, and HR).

**Implement Information Security Program Requirements for the Gramm-Leach-Bliley Act**
**Management Response:** The UVA Academic Division concurs with the APA's finding.
**Responsible for Corrective Action:** Steve Kimata, Assistant VP Student Financial Services; Jason Belford, Chief Information Security Officer
**Anticipated Completion Date:** June 2023

The University will develop a plan to comply with all GLBA requirements. This will include identifying the relevant systems and contracting with a third-party servicer to conduct comprehensive risk assessments in compliance with GLBA requirements.

The timeframe for compliance with the identified systems will likely extend into calendar year 2023; for example, the assessments will need to include the new Finance system that the University is implementing July 1, 2022. The contractual arrangement with a vendor is expected to be completed in early 2022.

**Improve Controls over User Access to the Payroll and Human Resources System**
**Management Response:** UVA concurs with the APA's finding.
**Responsible for Corrective Action:** Augie Maurelli, AVP for Financial Operations; Teresa Wimmer, AVP for Enterprise Applications
**Anticipated Completion Date:** July 2022

The University agrees with the APA's recommendations on a resource to identify potential conflicting business processes and their respective roles.

The University is undergoing significant change to its finance system, including a completely new set of user roles requiring definition, and changes to requesting access. This system will require integration with the current Payroll and Human Resources system.

The University has been evaluating resources, and will be implementing a solution to identify, monitor, and audit potential conflicts and segregation of duties in real time. This solution will also provide an opportunity for the University to establish and implement enhanced controls within the provisioning process for user access requests. This solution will be part of the enterprise financials system conversion and will carry over to 2023 due to implementation and conversion of all interdependent systems.

*UVAFinance is the valued and trusted financial partner that the University community turns to first.*
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | F 434.982.2315 | vpfinance@virginia.edu

**UVA Wise SFA Management Points**
**Management Response**: UVA-Wise concurs with APA's finding, detailed responses provided separately.
**Responsible for Corrective Action**: Joe Kiser, Vice Chancellor for Finance – UVA Wise
**Anticipated Completion Date**: June 2022

UVA Wise reviewed the Management Points and recommendations issued following the completion of the audit of financial records and operations supporting the Student Financial Aid Federal program of the University of Virginia's College at Wise (UVA Wise), as of and for the fiscal year ended June 30, 2020, as part of the five (5) year reaccreditation process:

- MP01 - Improve Reporting to the Common Origination and Disbursement System (COD)
- MP02 - Improve Federal Direct Loan Borrower Notification Process
- MP03 - Ensure Student Status Changes are Reported Accurately and Timely
- MP04 – Properly Manage Return of Title IV Funds
- MP05 - Promptly Return Unearned Title IV Funds to Department of Education
- MP06 - Ensure an Accurate FISAP is Submitted to Department of Education
- MP07 - Perform Federal Direct Loan Reconciliations Timely
- MP08 - Enhance Notification for Borrowers that have not Completed Exit Counseling
- MP09 - Improve Direct Loan Quality Assurance Program
- MP10 - Strengthen Compliance with the Gramm-Leach-Bliley Act

Although the findings do not constitute a material weakness, UVA Wise agrees that the issued management points around internal controls and compliance with applicable laws, regulations, contracts, and grant agreements should be addressed as required and appropriate. UVA Wise will engage with central offices of UVA Finance and Student Financial Services at the University of Virginia to establish additional procedures and plans for continuous monitoring.

UVA Wise has provided detailed corrective action plans that will be included in full in the statewide report.

*UVAFinance is the valued and trusted financial partner that the University community turns to first.*
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | F 434.982.2315 | vpfinance@virginia.edu

**MEDICAL CENTER**

**Security Awareness Training**

**Management Response:** The Medical Center concurs with the APA's finding.
**Responsible for Corrective Action**: Robin Parkins, Chief Information Officer Medical Center; Phil Napier, UVA Health Information Security Officer; Adam Weikel, Assistant VP of HR Service
**Anticipated Completion Date**: June 2022

Information Security will partner with UVA Human Resources to strengthen current practices associated with our annual mandatory training, which contains the Security Awareness Training (SAT). HR will coordinate an effort to ensure all outstanding team members have completed the training prior to January 31, 2021, with explicit communication noting sanctions for non-compliance, as well as detailed instructions for managers. For fiscal year 2022, all employees will need to complete SAT training prior to May 2022. IT will establish designated security roles, System Owners, Data Owners, etc. and define an appropriate cadence for ongoing role-based training associated with these roles. Content for training modules associated with role-based training will be developed by June 2022 and implemented in fiscal year 2023.

**Improve Firewall Patch Management**

**Management Response:** The Medical Center concurs with the APA's finding.
**Responsible for Corrective Action:** Robin Parkin, Chief Information Officer Medical Center; Phil Napier, UVA Health Information Security Officer
**Anticipated Completion Date:** March 2022

The UVA Medical Center's Information Technology Infrastructure Team will establish an internal process wherein any releases of new firewall versions that UVA Medical Center does not intend to apply be documented by a risk analysis approach. For these release versions or patches, a security exception will be submitted with the risk analysis and members of HIT Senior Leadership teams executing the review of the security exception. The exception will be authorized by an appropriate level of sign off based on the risk posed to the organization.

**Improve Accuracy of Provider Relief Fund Reporting**

**Management Response:** The Medical Center concurs with the APA's finding regarding provider relief federal fund compliance as related to the PRF reporting as required by the Health Resources & Services Administration (HRSA) report.
**Responsible for Corrective Action:** Brian Wilmoth, Chief Reimbursement Officer; Doug Lischke, UVA Health Chief Financial Officer; Kim Holdren, Director of Finance and Controller
**Anticipated Completion Date:** April 2022

*UVAFinance is the valued and trusted financial partner that the University community turns to first.*
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | F 434.982.2315 | vpfinance@virginia.edu

The Medical Center concurs with the APA's finding regarding provider relief federal fund reporting as required by the Health Resources & Services Administration (HRSA) report.

In order to correct and prevent further errors, the Medical Center will take the following steps:

- For future reporting periods, the Medical Center will correct the revenue and expenditure classification. HRSA has specifically stated that the 6/30/2020 filing cannot be amended.
- The Medical Center will continue to have a third party review the HRSA submission before entering into the portal.

**Allocate Additional Resources for Financial Statement Preparation**
**Management Response:** The Medical Center concurs with APA's finding to allocate additional resources to financial statement presentation.
**Responsible for Corrective Action:** Kim Holdren, Director of Finance and Controller
**Anticipated Completion Date:** June 2022

The Medical Center concurs with APA's finding to allocate additional resources to financial statement presentation. In response to the APA's finding, the Medical Center will take the following proactive steps:

- Identify external expertise to assist with financial reporting:
  - GASB interpretation and application when standards change, or new standards are issued
  - Impact, if any to the Medical Center regarding the statements and disclosures, to include guidance and examples for Medical Center personnel to apply when preparing the annual financial statements
  - To streamline and improve the overall Medical Center financial statement package
- Assuming budgeted dollars are available, the Controller's Office plans to seek additional professional accounting staff, in order to allow the Controller and Assistant Controller more time for review during the daily, monthly, and annual reconciliation and financial statement preparation process

*UVAFinance is the valued and trusted financial partner that the University community turns to first.*
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | F 434.982.2315 | vpfinance@virginia.edu

Sincerely,

DocuSigned by:
Melody Bianchetto
6F94A4B8D47A47D...
Melody Bianchetto
Vice President for Finance

cc: J.J Davis
Augie Maurelli
Virginia Evans
John Kosky

DocuSigned by:
Douglas E. Lischke
483FC542917C4DF...
Douglas E. Lischke
Health System Chief Financial Officer

cc: Kim Holdren
Wendy Horton
Erin Trost
Mike Marquardt

*UVAFinance is the valued and trusted financial partner that the University community turns to first.*
Carruthers Hall | 1001 N Emmet Street | PO Box 400210 | Charlottesville, VA 22904-4210
P 434.924.0716 | F 434.982.2315 | vpfinance@virginia.edu

## UNIVERSITY OF VIRGINIA

As of June 30, 2021

### BOARD OF VISITORS

James B. Murray, Jr.
Rector

Whittington W. Clement
Vice Rector

Robert M. Blue
Mark T. Bowles
L.D. Britt
Frank M. Conner, III
Elizabeth M. Cranwell
Thomas A. DePasquale
Barbara J. Fried
John A. Griffin
Louis S. Haddad
Robert D. Hardie
Maurice A. Jones
Babur B. Lateef
Angela H. Mangano
C. Evans Poston, Jr.
James V. Reyes

Sarita Mehta
Student Representative

Ellen M. Bassett
Faculty Representative

Susan G. Harris
Secretary to the Board of Visitors

### ADMINISTRATIVE OFFICERS

James E. Ryan
President

Jennifer Wagner Davis
Executive Vice President and Chief Operating Officer