



# VIRGINIA STATE UNIVERSITY

## REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2024

Auditor of Public Accounts

Staci A. Henshaw, CPA

[www.apa.virginia.gov](http://www.apa.virginia.gov)

(804) 225-3350



## AUDIT SUMMARY

We have audited the basic financial statements of Virginia State University (University) as of and for the year ended June 30, 2024, and issued our report thereon, dated August 28, 2025. Our report, included in the University's basic financial statements, is available at the Auditor of Public Accounts' website at [www.apa.virginia.gov](http://www.apa.virginia.gov) and at the University's website at [www.vsu.edu](http://www.vsu.edu). Our audit found:

- the financial statements are presented fairly, in all material respects;
- two internal control findings requiring management's attention; however, we do not consider them to be material weaknesses;
- six matters involving internal control and its operation necessary to bring to management's attention that also represent instances of noncompliance with applicable laws and regulations or other matters that are required to be reported; and
- adequate corrective action with respect to prior audit findings and recommendations identified as complete in the [Findings Summary](#) included in the Appendix.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendation.

Our audit also included testing over the major federal program of the Student Financial Assistance Programs Cluster 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 -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-10
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	11-13
APPENDIX – FINDINGS SUMMARY	14
UNIVERSITY RESPONSE	15-17

## INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

### **Improve Financial Reporting and Internal Controls over Capital Assets**

**Type:** Internal Control

**Severity:** Significant Deficiency

Virginia State University (University) lacks adequate internal controls over capital assets necessary for accurate management and financial reporting of capital assets in the financial statements. As indicated in our “Improve Policies and Procedures” internal control finding and recommendation below, the University needs to strengthen its policies and procedures for properly capitalizing assets; managing disposals; identifying, assessing, valuing, and reporting leases and subscription-based information technology arrangements; conducting physical inventories; and handling other capital asset related matters which are necessary to ensure that the University adheres to Governmental Accounting Standards Board (GASB) standards. Due to the University’s decentralized structure, the Financial Services Department (Financial Services) depends on the Auxiliary Services Department (Auxiliary Services) and various custodial departments to identify, record, track, and report capital asset activities throughout the year. The absence of sufficient policies, procedures, internal controls, and resources has led to the following deficiencies:

- Auxiliary Services did not perform a physical inventory in fiscal year 2024 and has not performed a complete physical inventory since fiscal year 2018. During our review, we selected 40 assets from the University’s system asset listing, of which 8 (20%) were improperly tagged or unable to be located. In addition, we selected 38 assets identified on campus and noted ten (26%) improperly tagged or unable to be located on the system asset listing. We also found 11 out of 20 (55%) assets selected were not capitalized correctly and/or timely and that one out of four (25%) was not entered into the system. Financial Services also improperly recorded retainage payable.
- Financial Services did not properly record amounts related to agreements made with component units, leases, public-private partnerships, and group asset purchases. Financial Services also did not accurately evaluate two leases, resulting in an understatement of approximately \$8.5 million in lease liabilities, \$9.7 million in net depreciable capital assets, \$2 million in operating expenses, and \$229,000 in non-operating expenses. Lastly, Financial Services and Auxiliary Services did not capitalize all group asset purchases as newly required by GASB, resulting in an understatement of approximately \$2 million in capital asset beginning balances and beginning net position.
- The University implemented a new capital asset management system within its accounting and financial reporting system; however, insufficient training and processes resulted in several financial statement adjustments. University staff were not fully trained on the functionality of the new system and therefore did not accurately record capital asset transactions. As part of its year end accounting procedures, Financial Services performed a reconciliation between the University’s accounting and financial reporting system finance

module and the new capital asset module. This reconciliation was not performed timely and reconciling differences were not fully researched, resulting in a misstatement of net depreciable capital assets of approximately \$700,000 and a misstatement in the capital assets footnote of \$387,000.

University Management is responsible for designing, implementing, and maintaining internal controls relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement in accordance with generally accepted accounting principles. The lack of adequate internal control processes over capital asset financial reporting increases the risk that users of financial statements may draw improper conclusions about the University's financial activities.

The deficiencies above are attributable to certain inadequately designed controls and insufficiently documented policies and procedures compounded by staff turnover in key positions, and the implementation of new GASB standards. In addition, the University began using the capital asset module within its accounting and financial reporting system as the system of record for capital asset reporting and is in the process of implementing an inventory control system.

The University should implement adequate internal controls for managing and safeguarding capital assets. In addition, it should develop, execute, and maintain effective policies and procedures, and controls, over all capital asset areas to ensure compliance with GASB standards and to align with University and Commonwealth best practices. Moreover, the University should provide Auxiliary Services and the various departments with training to enable Financial Services to accurately identify, evaluate, and report pertinent capital asset information.

### **Improve Policies and Procedures**

**Type:** Internal Control

**Severity:** Significant Deficiency

The University lacks adequate policies and procedures over certain financial reporting and operational areas. During our review, which focused on comprehensive financial policies and procedures, we found the University did not have formalized, complete, and/or up-to-date policies and procedures in specific areas. Existing guidance is outdated, insufficiently detailed, or did not reflect the University's current practices and systems and did not include some requirements contained within Commonwealth of Virginia standards or GASB standards.

Comprehensive financial reporting policies and procedures are essential to promoting transparency, accountability, compliance, and accuracy in financial reporting. During the audit, we identified financial statement adjustments that were attributable to deficiencies in the University's financial reporting policies and procedures. The adjustments highlight the need for a formalized and consistently applied framework and review process to ensure accuracy and reduce the risk of misstatements in the financial statements. An effective financial reporting framework includes, but is not limited to, policies and procedures addressing the following areas:

- Adoption and adherence to applicable standards
- Ongoing evaluation and implementation of new standards or updates, including assessing any applicability and operational impact
- Documentation and internal review of nonroutine, judgment-based, or complex transactions to ensure appropriate treatment and consistency
- Performance of timely, accurate, and documented reconciliation processes
- Processes to ensure all required elements are included in note disclosures and required supplementary information (RSI) and updated annually
- Review of disclosures and RSI for consistency with standards and the financial statements

As noted in Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 20905, a lack of complete and up-to-date internal policies and procedures, customized to reflect the agency's staffing, organization, and operating procedures, reflects inadequate internal control. These deficiencies primarily stem from a lack of a formalized plan to periodically review and update policies and procedures.

The University should evaluate current financial reporting policies and procedures for sufficiency. We recommend the University develop a plan to review and update policies and procedures prioritizing financial reporting, higher-risk operational areas, and areas where the University has experienced more significant changes in operations since the last policy and procedure update period. Where the University identifies inadequacy in its policies and procedures, it should modify existing or develop new policies and procedures, as applicable, and disseminate those policies and procedures to University staff for implementation. A comprehensive review and update of the University's outdated policies and procedures will take time and resources; however, developing a plan and timeline will enable the University to focus on the most critical areas and provide accountability for making progress in this endeavor. Additionally, moving forward, management should implement a schedule for periodic review and update of all policies and procedures to ensure they reflect changes in processes, systems, and standards.

### **Improve Access and Account Management Controls**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Reported:** Fiscal Year 2020

The University's Information Security Office (Information Security) did not remove systems access in a timely manner for terminated employees, nor did it retain documentation supporting timely system access removal for three University systems. During our review, we found:

- Information Security did not retain documentation indicating when staff removed access to the University’s accounting and financial reporting system upon employee termination for 11 employees.
- Information Security did not retain documentation indicating when staff removed access to the University’s residential housing system upon employee termination for four employees.
- Information Security did not remove access to the University’s accounting and financial reporting system timely for two employees.
- Information Security did not remove access to the Commonwealth’s purchasing system timely for two employees.

The Commonwealth’s Information Security Standard, SEC530 (Security Standard) requires agencies to "disable information system access within 24 hours of employment termination." CAPP Manual Topic No. 21005 – Records Retention and Disposition outlines the requirements for document retention, requiring agencies to “ensure that records are preserved, maintained, and accessible throughout their lifecycle.” Not retaining documentation that shows timely system access removal, especially for former employees or contractors, can increase the risk of noncompliance with the Security Standard. Not removing system access timely increases the risk of unauthorized access to sensitive data by individuals no longer employed by the University.

Resource limitations in Information Security as well as management oversight contributed to these deficiencies. Over the past year, the University ensured that staff performed the required annual reviews of privileges assigned to users. The University is in the process of implementing a new single sign-on solution to assist with account management, which should allow Information Security to remove access to University information systems in a more automated fashion. Where possible, Information Security should incorporate all applicable systems within the new single sign-on solution. The University should implement processes and dedicate the necessary resources to ensure Information Security retains sufficient documentation of access removal, as well as timely removes systems access.

**Improve IT Risk Management and Contingency Planning Program**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

The University does not manage its information technology (IT) risk management and contingency planning program in accordance with University policies, as well as the Security Standard. The following five weaknesses exist:

- The University does not maintain an accurate IT Systems and Data Sensitivity Classification. While the University properly assigned a rating of low, medium, or high to the confidentiality, integrity, and availability of each dataset, the University did not classify four of its datasets as sensitive despite all four datasets having a rating of ‘high’ in one or more categories of confidentiality, integrity, and availability. The University’s Risk Management and IT System

and Data Sensitivity Policy (Risk Management Policy) states that the University should appropriately classify data sensitivity and should classify IT systems or applications as sensitive if any type of data it processes has a sensitivity of 'high' for confidentiality, integrity, or availability. The Security Standard states that the University should classify systems as sensitive if a type of data handled has a sensitivity of moderate for two or more categories or high for one or more of the categories of confidentiality, integrity, or availability, and verify that all University IT systems and data have been reviewed and classified as appropriate for sensitivity. Failure to properly classify IT systems and data could result in a potential compromise of the University's sensitive data and information due to inadequate risk management documentation.

- The University's Continuity of Operations Plan (COOP) and IT Disaster Recovery Plan (IT DRP) do not align with the University's updated Business Impact Analysis (BIA). As such, the University COOP and IT DRP have Mission Essential Functions (MEFs) and Primary Business Functions (PBFs) that do not accurately reflect the MEFs and PBFs identified in the University's updated BIA. The University's Business Impact Analysis Policy requires that the University develop a BIA and based on the results of the BIA, develop IT disaster recovery components of the COOP, and periodically review, reassess, test, and revise the COOP and IT DRP to reflect changes in essential business functions. The Security Standard states that the University should, based on the BIA and risk assessment (RA) results, develop IT disaster components of the COOP. Failure to align the University's COOP and IT DRP based on the results of the BIA could result in inaccurate disaster recovery and contingency planning information, which could prevent the University from properly executing its contingency planning procedures in the event of an activation of the COOP and IT DRP.
- The University has not completed a RA for three of its four (75%) sensitive IT systems. The University's Risk Management Policy requires that the University Information Security Officer, in collaboration with system owners and data owners, conduct and document RAs for each sensitive IT system every three years, or sooner if needed, and that system owners review RAs annually. The Security Standard states that the University should conduct a RA for each sensitive system, review RA results on at least an annual basis, and update the RA on an annual basis or when significant changes occur. Not completing and regularly updating RAs as necessary for each sensitive IT system could result in potential unrecognized risks and compromise of the University's sensitive IT systems and data.
- The University has not completed a system security plan (SSP) for three of its four (75%) sensitive IT systems. The University's Systems Security Plan and Systems Operability Agreement Policy (SSP Policy) states that the system owner of each University system classified as sensitive shall use the results of the BIA and RA to develop a formal SSP for each sensitive IT system. The SSP Policy also states that the system owner should conduct periodic reviews to determine the continued validity of the SSP and update the SSP as needed based on environmental changes. The Security Standard states that the University should document an IT SSP for the IT system based on the results of the RA, that should include all existing and planned IT security controls for the IT system, and how these controls provide

adequate mitigation of risks to which the IT system is subject. Without a complete SSP for each of the University's sensitive IT systems, the University cannot adequately plan and map security controls for its IT systems, which could result in potential unidentified risks to the University's sensitive systems and information.

- The University does not test the COOP annually to determine if significant IT resources identified in the COOP can be obtained in the event of COOP activation. The University's Contingency Planning Policy requires that the University perform an exercise, at least annually, of the University COOP and IT DR components to assess the adequacy and effectiveness of the plan and then review and revise the COOP following the exercise. The Security Standard requires that the University perform an annual exercise of IT disaster recovery components of the COOP to assess their adequacy and effectiveness, and review and revise the COOP following the exercise. In addition, the Security Standard requires that the University test the COOP on an annual basis and following an environmental change, review the test results, and initiate corrective actions if needed. By not testing the COOP annually, the University cannot ensure that the necessary IT resources needed to support contingency procedures can be recovered in the event of an activation of the COOP, which may result in the potential inability to obtain these resources in the event of a disaster.

The University, in conjunction with the Virginia Information Technologies Agency (VITA) Centralized Information Security Officer Security Services (ISO Services), completed a new BIA and IT Systems and Data Sensitivity Classification during calendar year 2024. The University is currently engaged with VITA's ISO Services to complete RAs and SSPs for all sensitive IT systems but has not completed the process due to lack of resources. The University delayed updating the COOP, performing an annual COOP test, and updating the IT DRP until after VITA completes the RA and SSPs.

The University should ensure it maintains an accurate IT Systems and Data Sensitivity Classification and classifies all University IT systems and data as appropriate according to the categories of confidentiality, integrity, and availability. The University should also complete an RA and SSP for each IT system classified as sensitive and update the University's COOP and IT DRP to accurately reflect the University's environment. Finally, the University should ensure it conducts a COOP test annually, documents lessons learned from the test, and updates the COOP accordingly. Improving the University's IT risk management and contingency planning program will help ensure the University protects the confidentiality, integrity, and availability of its sensitive and mission-critical IT systems and data.

### **Improve Router Security**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Reported:** Fiscal Year 2023

The University does not secure the routers that support its network in accordance with the Security Standard. The routers are critical network infrastructure components used to route and manage traffic within the University's network. The University made progress to improve security over the router

by updating its Password Management Policy to meet the password character length requirements of the Security Standard; however, two weaknesses from the prior year remain:

- The University does not patch the router within 30 days of release of the updates. The Security Standard requires that the University install security-relevant software and firmware updates within at least 30 days of release of the updates. Running an outdated operating system exposes the routers to security vulnerabilities that could result in malicious actors compromising the University’s sensitive network and information. The University is currently in the process of documenting procedures to require and implement a process to apply patches within 30 days of release.
- The University does not scan routers monthly for vulnerabilities, and as a result does not subsequently remediate identified vulnerabilities within 30 days as required by the Security Standard. The Security Standard requires that the University scan for vulnerabilities every 30 days and remediate legitimate vulnerabilities within 30 days in accordance with an organizational assessment of risk. Failure to perform vulnerability scans and subsequently remediate legitimate vulnerabilities over the routers could result in potential exploitation of those vulnerabilities and compromise of the University’s sensitive network and information.

The University did not patch the router within 30 days of release of the updates due to the lack of a policy requirement to apply patches within 30 days of release. The University did not scan the routers as it was in the process of transitioning to a new scanning solution. As of July 1, 2023, the University implemented a VITA solution provided at no cost to the University. The University discovered after the implementation that the platform lacked the capability of scanning internal infrastructure, including the University’s routers. In May 2024, the University decided to procure a scanning solution to scan internal infrastructure. The University procured the scanning solution in December 2024 but has not yet fully configured the scanning solution to scan the routers.

The University should update its policy to require patches to be applied within 30 days of release. Additionally, the University should configure the scanning solution to scan its routers, conduct monthly vulnerability scans, and remediate legitimate vulnerabilities within 30 days, as required by the Security Standard. Improving router security will help protect the University from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data.

**Engage and Use COV Ramp to Provide Required Active Oversight**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Reported:** Fiscal Year 2023

**Prior Title:** Engage and Use ECOS to Provide Required Active Oversight

The University continues to not properly gain assurance over outsourced operations of IT third-party service providers (providers) that required oversight by VITA’s COV Ramp Oversight Services (COV Ramp). The University uses six providers for mission-critical business functions that require oversight by COV Ramp to protect the Commonwealth and the University. The University is proactively obtaining and

reviewing System and Organization Controls reports annually for each of the six providers independent of the COV Ramp oversight process and developed a procedure to facilitate the oversight process. For three of the University's six providers, the University continued to not meet the oversight requirements of the Security Standard due to not completing the necessary steps required to obtain active oversight by COV Ramp.

The Security Standard and the University's System and Services Acquisition Policy require that the University employ appropriate processes, methods, and techniques to monitor security control compliance by external providers on an ongoing basis. The University's Third-Party Supplier Oversight Process requires the University to complete the appropriate steps to achieve COV Ramp Oversight for the providers that qualify. The Security Standard states that management remains accountable for maintaining compliance with the Security Standard through documented agreements with providers and oversight of the services provided.

By not properly requesting active oversight for all the University's providers that qualified for COV Ramp oversight during fiscal year 2024, the University cannot ensure that providers have effective information security controls to protect the University's sensitive and confidential data and ensure mitigation of control deficiencies. Undetected, ineffective provider controls increase the chance of a breach or possible data disclosure. The University did not request active COV Ramp oversight for three of its six providers that qualify due to management oversight. Additionally, since the University received additional autonomy from the Commonwealth through recognition of tier 2 status in fiscal year 2025, the University is in the process of transitioning from COV Ramp Oversight to an internal provider oversight process.

The University should comply with the provider oversight requirements of the Security Standard for all of its providers, whether through active COV Ramp oversight or the University's own oversight activities and processes. Obtaining appropriate oversight of its providers will help protect the University from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data.

### **Improve IT Policies and Procedures**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

The University does not ensure that its IT policies and procedures align with the requirements of the Security Standard. Specifically, the following three weaknesses exist:

- The University does not have documented procedures to facilitate the implementation of University policies for the following 13 control families as required by the Security Standard:
  - o Access Control
  - o Assessment, Authorization, and Monitoring
  - o Configuration Management
  - o Contingency Planning
  - o Identification and Authentication
  - o Maintenance
  - o Media Protection

- o Physical and Environmental Protection
- o Planning
- o Personnel Security
- o Risk Assessment
- o System and Communications Protection
- o System and Information Integrity

The Security Standard requires that the University develop, document, and disseminate topic-specific procedures to facilitate the implementation of each required IT policy and the associated controls, and review and update the current procedures on an annual basis and following an environmental change. Failure to develop and document procedures to facilitate the implementation of the University's IT policies could result in the University failing to define a process to implement specific control requirements, which could expose the University to possible compromise of its sensitive IT environment and data.

- The University's System Information and Integrity Policy (System Information Policy) does not align with the requirements of the Security Standard. Specifically, the System Information Policy requires that the University remediate flaws by installing security-relevant software and firmware updates within 90 days of the release of the updates, instead of within 30 days of release as required by the Security Standard. By not requiring the installation of security-relevant software and firmware updates within 30 days of release, the University risks possible outdated software and firmware on critical systems and infrastructure, which may result in exploitable vulnerabilities remaining in the University's environment.
- The University developed a Technology Policy Development and Maintenance Standard (Technology Standard) that does not align with the requirements of the Security Standard. Specifically, the Technology Standard states that the University will review procedures at a minimum of every three years and does not require a review of policies, while the Security Standard requires the review of policies and procedures for each control family be on at least an annual basis. Failure to review and update policies and procedures at least annually could result in outdated procedures that do not accurately reflect the University's process for implementing required controls, which could increase exposure to malicious actors or errors.

The University does not have documented procedures for each University IT policy due to lack of management oversight and staff. Additionally, both the University's System Information Policy and its Technology Standard do not align with the Security Standard due to insufficient management oversight.

The University should develop procedures to ensure the implementation of each IT policy and the related controls. The University should also update both its System Information Policy and Technology Standard to align each with the requirements of the Security Standard and review each IT policy and procedure annually as required by the Security Standard. Improving the University's IT policies and procedures will help ensure the confidentiality, integrity, and availability of the University's sensitive and mission-critical data and environment.

## **Improve Reporting to National Student Loan Data System**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Reported:** Fiscal Year 2018

**Prior Title:** Report Student Status Enrollment Changes Accurately and Timely to National Student Loan Data System

University personnel did not report accurate and timely enrollment data to the National Student Loan Data System (NSLDS) for students that graduated, withdrew, or had an enrollment level change. Inadequate management oversight and a lack of effective processes to ensure data accuracy and compliance with reporting requirements contributed to the deficiencies identified. From our sample of 49 students, we noted the following instances of noncompliance:

- inaccurate enrollment status reported for three students (6%);
- inaccurate effective date reported for six students (12%);
- untimely reporting of enrollment status changes for 21 students (43%);
- inaccurate reporting of at least one field deemed critical at the campus or program level for ten students (20%);
- inability to verify approval of the student's academic program for eight students (16%), since it did not appear on the State Council of Higher Education for Virginia's Degree Inventory Report; and
- conflicting addresses for two out of 39 applicable Federal Direct Loan borrowers (5%) between the University's student information system and the NSLDS Student Contact Information screen.

In accordance with Title 34 U.S. Code of Federal Regulations (CFR) § 690.83(b)(2) an institution shall submit, in accordance with deadline dates established by the Secretary, other reports and information the Secretary requires and shall comply with the procedures the Secretary finds necessary to ensure the reports are correct. As further outlined in the NSLDS Enrollment Guide, published by the U.S. Department of Education (ED), at a minimum, institutions are required to certify enrollment every 60 days. The accuracy of Title IV enrollment data depends heavily on information reported by institutions. The University's inaccurate and untimely enrollment data submissions to the NSLDS can affect ED's reliance on the system for monitoring purposes. Noncompliance may also impact an institution's participation in Title IV programs.

University management should evaluate its current enrollment reporting desk procedures and implement corrective action to ensure that the University reports accurate and timely student enrollment status changes to the NSLDS. Management should also consider implementing a quality control review process to monitor the accuracy of campus and program level batch submissions.



# Commonwealth of Virginia

*Auditor of Public Accounts*

Staci A. Henshaw, CPA  
Auditor of Public Accounts

P.O. Box 1295  
Richmond, Virginia 23218

August 28, 2025

The Honorable Glenn Youngkin  
Governor of Virginia

Joint Legislative Audit  
and Review Commission

Board of Visitors  
Virginia State University

Makola Abdullah  
President, Virginia State University

## **INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS**

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of **Virginia State University** (University) as of and for the year ended June 30, 2024, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated August 28, 2025. Our report includes a reference to other auditors who audited the financial statements of the component units of the University, as described in our report on the University's financial statements. The other auditors did not audit the financial statements of the component units of the University in accordance with Government Auditing Standards, and accordingly, this report does not include reporting on internal control over financial reporting or compliance and other matters associated with the component units of the University.

### **Report on 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 Financial Reporting and Internal Controls over Capital Assets," "Improve Policies and Procedures," "Improve Access and Account Management Controls," "Improve IT Risk Management and Contingency Planning Program," "Improve Router Security," "Engage and Use COV Ramp to Provide Required Active Oversight," "Improve IT Policies and Procedures," and "Improve Reporting to National Student Loan Data System," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

### **Compliance and Other Matters**

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the 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 section titled "Internal Control and Compliance Findings and Recommendations" in the findings and recommendations titled "Improve Access and Account Management Controls," "Improve IT Risk Management and Contingency Planning Program," "Improve Router Security," "Engage and Use COV Ramp to Provide Required Active Oversight," "Improve IT Policies and Procedures," and "Improve Reporting to National Student Loan Data System."

### **The University's Response to Findings**

We discussed this report with management at an exit conference held on September 8, 2025. Government Auditing Standards require the auditor to perform limited procedures on the University's response to the findings identified in our audit, which is included in the accompanying section titled "University Response". The University's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

### **Status of Prior Findings**

The University has not taken adequate corrective action with respect to the prior reported findings identified as ongoing in the Findings Summary included in the Appendix. The University has taken adequate corrective action with respect to prior audit findings and recommendations identified as complete in the [Findings Summary](#) included in the Appendix.

### **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

AVC/vks

## FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Improve Service Provider Oversight	Complete	2020
Promptly Return Unclaimed Aid to Department of Education	Complete	2021
Improve Financial Reporting Review Process	Complete	2022
Improve Financial Reporting and Internal Controls over Capital Assets	Ongoing	2024
Improve Policies and Procedures	Ongoing	2024
Improve Access and Account Management Controls	Ongoing	2020
Improve IT Risk Management and Contingency Planning Program	Ongoing	2024
Improve Router Security	Ongoing	2023
Engage and Use COV Ramp to Provide Required Active Oversight**	Ongoing	2023
Improve IT Policies and Procedures	Ongoing	2024
Improve Reporting to National Student Loan Data System***	Ongoing	2018

\* A status of **Complete** indicates management has taken adequate corrective action. A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

\*\* The prior title of this finding was "Engage and Use ECOS to Provide Required Active Oversight."

\*\*\* The prior title of this finding was "Report Student Status Enrollment Changes Accurately and Timely to National Student Loan Data System."



# VIRGINIA STATE UNIVERSITY

P.O. Box 9031

Virginia State University, Virginia 23806-0001

Kevin W. Davenport, Senior Vice President  
Administration and Finance, and CFO

Phone: (804) 524 - 5995

September 23, 2025

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

Dear Ms. Henshaw:

Virginia State University appreciates the Auditor of Public Accounts' work and the brevity of the report. Fiscal Year 2024 was a deliberate year of modernization: we implemented Banner Fixed Assets as our fixed-asset subledger of record, strengthened identity and access processes, aligned information technology risk practices to an updated Business Impact Analysis, and tightened federal student aid reporting. Our responses below reflect actions already operating. Each matter will be considered closed when evidence shows that residual risk is at or below the University's established, documented standards.

### **Improve Financial Reporting and Internal Controls over Capital Assets**

Concur. The adjustments identified are consistent with first-year adoption of recent Governmental Accounting Standards Board requirements—such as leases and Subscription-Based Information Technology Arrangements—as well as the conversion to the Banner Fixed Assets subledger. Many public universities experienced similar transition-year variances while modernizing fixed-asset systems and measuring right-to-use assets. These are normal effects of modernization, not indicators of control failure.

What is in place and advancing in our modernization efforts: Banner Fixed Assets is the system of record; monthly ties between the subledger and the general ledger are operating; a lease and subscription intake process includes controller review; and a campus-wide inventory with re-tagging and documented disposals is underway. Valuation memoranda (including discount rates, lease terms, and grouping logic) support complex accounting judgments. These controls reduce post-close adjustments and sustain accurate, timely capital reporting.

### **Improve Policies and Procedures**

Partially Concur. VSU agrees that regular evaluation and improvement of policies and procedures is sound practice. We will continue to prioritize updates to financial reporting policies in alignment with Governmental Accounting Standards Board (GASB) requirements and Commonwealth guidance. At the same time, we disagree that the absence of fully updated policy language across every operational area, by itself, constitutes an internal control failure. In this audit, no material weaknesses were identified, and policy observations were not shown to have caused material errors or misstatements.

GREATER HAPPENS HERE

# VIRGINIA STATE UNIVERSITY

P.O. Box 9031

Virginia State University, Virginia 23806-0001

Moreover, the noted financial statement adjustments reflect prudent, timely refinements made during the audit—not indicators of failed control. The finding does not link specific outdated or incomplete policy language to a discrete instance of misreporting or noncompliance. Commonwealth Accounting Policies and Procedures (CAPP) guidance contemplates risk-based tailoring of procedures; alignment to risk remains our focus.

We will continue to refresh policy documents so they mirror practices already in operation, with emphasis on areas of highest financial risk, and appreciate the guidance provided in our continuous process improvement efforts.

### **Improve IT Risk Management and Contingency Planning Program**

VSU concurs and acknowledges the timing delays in realigning risk assessments and contingency plans following IT system transitions and organizational shifts. Three of the four sensitive systems now have updated risk assessments and system security plans. Furthermore, the University's move to Level 2 oversight grants the internal CISO greater agility to maintain updated classifications and protocols in accordance with NIST 800-53. A new Director of IT Governance, Risk & Compliance has been hired to lead these initiatives, and integration between business impact analyses and continuity plans is underway.

### **Improve Router Security**

VSU concurs and notes that substantial progress has been made. The University adopted a new scanning solution after identifying limitations in the initial VITA-provided tool. While full router scanning configuration was not completed as of the audit period, the University has since accelerated deployment and revised internal policies to align with SEC530 standards. We appreciate APA's recognition of our password policy updates and will continue to strengthen patch management and vulnerability response timelines.

### **Improve Third-Party Oversight**

The University concurs and has taken steps to integrate third-party service provider oversight into vendor intake and contract renewal processes. We have updated our third-party inventory and aligned it with required security assessments. The Office of Procurement and IT are collaborating to ensure that data classification, sensitivity reviews, and security terms are embedded within contracting workflows.

### **Improve Financial Aid Compliance**

VSU concurs and notes that corrective actions are underway to fully automate enrollment change reporting to the National Student Loan Data System (NSLDS). Timing gaps occurred due to delays in student record updates and institutional staff transitions, not due to lack of process or oversight. The Financial Aid Office has implemented reconciliation checkpoints and is working closely with the Registrar to ensure real-time status accuracy.

# VIRGINIA STATE UNIVERSITY

P.O. Box 9031

Virginia State University, Virginia 23806-0001

## **Conclusion**

Virginia State University remains resolute in its mission of fiscal stewardship and operational excellence. The audit process is a critical partner in this endeavor, and we appreciate the APA's collaborative approach. We look forward to ongoing engagement, aligned interpretation of evolving standards, and timely closure of outstanding items.

Sincerely,



Kevin W. Davenport  
Senior Vice President for Administration and Finance  
and CFO

Cc: Dr. Makola M. Abdullah, President  
Aimee Rogstad Guidera, Secretary of Education  
Scott L. Adams, CPA, State Comptroller  
Michael Maul, Director of Planning and Budget