THE COLLEGE OF WILLIAM & MARY IN VIRGINIA

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2022

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the consolidated basic financial statements of The College of William & Mary in Virginia, as of and for the year ended June 30, 2022, and issued our report thereon, dated May 26, 2023. The consolidated basic financial statements of The College of William and Mary in Virginia include the financial activity of The College of William and Mary in Virginia (William & Mary), Virginia Institute of Marine Science, and Richard Bland College (Richard Bland), which report to the Board of Visitors of The College of William and Mary in Virginia. Our report, included in the consolidated basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at William & Mary's website at www.wm.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.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

RICHARD BLAND

Improve Firewall Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)

Richard Bland made limited progress since our last audit to secure its firewall in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard) and best practices. Richard Bland remediated two of the four weaknesses identified in the previous year's audit, but two weaknesses remain.

We communicated the control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The Security Standard and industry best practices require the implementation of certain controls to reduce unnecessary risk to confidentiality, integrity, and availability of Richard Bland's information systems and data.

Richard Bland experienced frequent staffing changes and turnover in the last year within the Information Technology (IT) Department, including the Information Security Officer position, which delayed Richard Bland's corrective actions. Additionally, Richard Bland executed a contract during calendar year 2022 to transition certain IT functions to a third-party service provider to help alleviate staffing resource constraints, which also delayed its implementation of corrective action.

Richard Bland should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE in accordance with requirements of the Security Standard and best practices. Implementing the required controls will help Richard Bland to secure its network to protect its sensitive and mission-critical systems and data.

Develop and Implement a Service Provider Oversight Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)

Richard Bland has not documented formal policies and procedures or implemented related processes to monitor the effectiveness of external service providers (providers) that do not qualify for the Virginia Information Technologies Agency's (VITA) Enterprise Cloud Oversight Services (ECOS) on an ongoing basis. Additionally, Richard Bland does not have a formal documented process to manage its Software as a Service (SaaS) providers covered by VITA's ECOS. Providers are organizations that perform certain business tasks or functions on behalf of Richard Bland and the Commonwealth. Richard Bland

currently uses 36 providers for mission-critical business functions, some of which include the processing and storing of sensitive data.

The Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard), states that management remains accountable for maintaining compliance with the Hosted Environment Security Standard through documented agreements with providers and oversight of services provided. The Hosted Environment Security Standard also requires organizations to employ appropriate processes, methods, and techniques to monitor the effectiveness of the providers' security controls on an ongoing basis (*Hosted Environment Security Standard, sections: 1.1 Intent, SA-9 External Information System Services*). Additionally, Richard Bland signed a Memorandum of Understanding (MOU) with VITA that requires Richard Bland to review and approve all ECOS documentation to monitor compliance with the MOU.

Without a documented and established process to gain assurance over the internal controls of providers that do not qualify for VITA's ECOS service, Richard Bland cannot consistently validate that those providers have effective security controls to protect Richard Bland's mission-critical and confidential data. Without a formal process to obtain VITA's ECOS oversight services, and then review and maintain VITA's ECOS documentation, Richard Bland cannot validate whether its SaaS providers implement security controls that meet the requirements in the Hosted Environment Security Standard to protect sensitive and confidential data. Richard Bland was unable to develop and implement a provider oversight process during the current audit period due to frequent staffing changes and turnover in its IT Department, including the Information Security Officer position.

Richard Bland should develop, document, and implement a service provider oversight process and dedicate the necessary resources to request and evaluate annual security assessment reports from each provider that does not qualify for ECOS oversight to ensure the provider has effective operating controls to protect Richard Bland's sensitive data. During the evaluation, Richard Bland should identify control deficiencies, develop mitigation plans, and as needed, escalate issues of noncompliance. Further, Richard Bland should develop a formal process to procure VITA's ECOS oversight for all SaaS providers, monitor and maintain ECOS oversight to ensure the providers comply with the Hosted Environment Security Standard, and ensure that VITA's ECOS satisfies its requirements as stated in the MOU. Effective provider oversight will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

Improve Database Security

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Richard Bland has not implemented minimum security controls and processes to protect the database that supports its accounting and financial reporting system in accordance with its policies, the Security Standard, and industry best practices, such as the Center for Internet Security's Benchmark (CIS Benchmark). We communicated six control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security

mechanisms. The Security Standard and industry best practices, such as the CIS Benchmark, require Richard Bland to implement certain controls to reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

Richard Bland's lack of policies and procedures and a formal baseline configuration contributed to the identified weaknesses. Additionally, Richard Bland has experienced frequent staffing changes and turnover in its IT Department, including the Information Security Officer position.

Richard Bland should develop policies and procedures, and a formal baseline configuration, that align with the Security Standard and industry best practices, such as the CIS Benchmark. Richard Bland should then dedicate the necessary resources to address the weaknesses in the FOIAE communication. Implementing these security controls and processes to protect the database will help maintain the confidentiality, integrity, and availability of Richard Bland's sensitive and mission-critical data.

Improve IT Risk Management Program

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Richard Bland does not properly manage certain aspects of its IT risk management and contingency planning program in accordance with the Security Standard and the Commonwealth's IT Risk Management Standard, SEC 520 (IT Risk Management Standard). The IT risk management and contingency planning program provides the baseline for Richard Bland to recover and restore mission-critical and sensitive systems based on the college's identification, assessment, and management of information security risks. Risk management documents include Richard Bland's business impact analysis and IT system risk assessments. Contingency planning documents include Richard Bland's continuity of operations plan and disaster recovery plan.

We communicated three control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The Security Standard and IT Risk Management Standard both require the implementation of certain IT risk management and contingency planning controls to reduce unnecessary risk to data confidentiality, integrity, and availability for Richard Bland's sensitive systems.

Richard Bland was unable to effectively manage its IT risk management and contingency planning program due to frequent staffing changes and turnover in its IT Department, including the Information Security Officer position. Richard Bland should dedicate the necessary resources to align its IT risk management and contingency planning program with the Security Standard and IT Risk Management Standard to protect the confidentiality, integrity, and availability of sensitive and mission-critical data.

Improve Controls over Contract Administration and Management
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Richard Bland signed a five-year, $7 million contract in December 2021 to outsource its IT Department. The contract's effective date was March 2022, however, Richard Bland voided the contract prior to this date after VITA legal counsel notified the college that the contract required VITA's approval. Title 2.2-4303.01 of the Code of Virginia requires state public bodies to submit high-risk contracts for IT goods and services to VITA for review prior to awarding the contract. As this was the first contract of this nature attempted by Richard Bland, personnel were unaware of the requirement to obtain VITA's approval prior to awarding the contract.

Upon voiding the original contract, Richard Bland submitted and received approval for an interim contract that governed the arrangement during the last quarter of fiscal year 2022 until VITA approved a five-year agreement effective for fiscal year 2023. During the interim contract period reviewed during the audit, Richard Bland did not have sufficient processes in place to ensure adequate contract administration and monitoring in accordance with the VITA Buy IT Manual (VITA Manual). Specifically, we identified the following deficiencies:

- Richard Bland did not explicitly identify a contract administrator in writing.

- Richard Bland did not maintain documentation to support its evaluation and determination of price reasonableness following a change to the interim contract that resulted in a daily price increase of 41 percent per business day.

- Richard Bland did not maintain sufficient documentation to support active monitoring of contractor performance to ensure services the contractor performed and billed were in accordance with the contract deliverables prior to making payment.

Chapter 34.2.1 of the VITA Manual requires written assignment of contract administration expectations and identification of individuals responsible for each function. Chapter 34.1 of the VITA Manual speaks to the contract administrator's responsibility to maintain accurate and complete documentation including, but not limited to, contract modifications and actions, contractor and agency communications, deliverable transmittals and acceptance documents, and contractor performance reports, evaluations, and results. Various other sections within Chapter 34 of the VITA Manual detail requirements regarding monitoring and maintenance of documentation to support contractor performance, agency obligations, invoicing and payments, and acceptance of deliverables. The VITA Manual emphasizes that it is critical to ensure maintenance and accessibility of all contract administration documentation regarding contract actions, contractor performance, and agency performance should there be any claims or disputes regarding contract performance.

Richard Bland experienced turnover within key management positions in Finance, IT, and Procurement Departments, all of whom were involved with the contract administration of the

outsourced IT services. While the interim contract in place during fiscal year 2022 defined contract administration responsibilities and included mechanisms to monitor contractor performance, the previously mentioned turnover impacted Richard Bland's ability to maintain adequate documentation to support active monitoring of contractor performance. By not officially assigning a contract administrator and defining their responsibilities in accordance with the VITA Manual, Richard Bland cannot ensure that there is clear assignment and accountability related to contract administration and monitoring. Inadequate contract administration and monitoring of outsourced IT services increases Richard Bland's risk of noncompliance with the VITA Manual and IT noncompliance with respect to requirements of the Security Standard.

Richard Bland has made changes to its contract administration process during fiscal year 2023 after signing the final contract; however, Richard Bland should ensure it clearly assigns and communicates contract administration responsibilities in accordance with the VITA Manual. Such responsibilities should include evaluation and maintenance of documentation related to changes to the contract and monitoring of contractor performance.

Improve Federal Financial Aid Reconciliation Controls

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Richard Bland should improve its controls over the reconciliation of federal financial aid to ensure that data used in the reconciliation is complete. During fiscal year 2022, for two of the three months tested (67%), Richard Bland used incomplete data to reconcile disbursements within its internal accounting and financial reporting system to cash drawdowns from the federal G5 system for various federal financial aid programs, including the Federal Direct Loan (FDL), Federal Pell Grant, Federal Supplemental Education Opportunity Grant, and Federal Work Study programs. The use of incomplete data in these reconciliations led to the improper identification of reconciling items. Furthermore, as the previously mentioned data was incomplete, Richard Bland did not effectively reconcile FDL cash drawdowns and disbursements to the Common Origination and Disbursement System (COD).

Richard Bland has written policies and procedures for the federal financial aid reconciliation; however, these policies and procedures do not address reconciling cash drawdowns and disbursements to COD. In accordance with Title 34 U.S. Code of Federal Regulations (CFR) 685.300(b)(5), a school that participates in the FDL program should reconcile monthly the funds received from the G5 system with actual disbursement records submitted to COD. The School Account Statement (SAS) provided from COD details differences between the two systems as an Ending Cash Balance (ECB). The U.S. Department of Education's (Education) Student Financial Aid Handbook, Volume 4 Chapter 6, requires institutions to document and explain any ECB reported in the SAS, if applicable. Finally, Education's Student Financial Aid Handbook, Chapter 5, states that Pell Grant reconciliations should occur regularly, with a recommendation of at least monthly. Proper reconciliation includes an internal reconciliation comparing internal disbursements and drawdown transactions and an external reconciliation comparing internal transactions with COD.

The lack of an effective oversight and review process in the Richard Bland Office of Finance and Administration (Finance and Administration) resulted in several undetected errors in the reconciliation process. Because Finance and Administration personnel did not properly update date constraints when obtaining data, they used incomplete disbursement data in the reconciliation. Additionally, cash drawdown data from the G5 system was incomplete due to Finance and Administration personnel running reports prior to the end of the month and not properly keying all data from the G5 system report into the reconciliation. The use of incomplete data when reconciling federal financial aid increases the risk that Richard Bland will not detect and correct financial aid discrepancies in student accounts and decreases accountability over financial aid programs. Additionally, there is an increased risk that Richard Bland will not properly return unspent financial aid funds to Education.

Richard Bland should improve its review of the reconciliation of federal financial aid to ensure the use of complete disbursement and cash drawdown data from its internal accounting and financial reporting system and the G5 system. Further, Richard Bland should ensure that policies and procedures sufficiently outline reconciliation requirements, to include the reconciliation to COD as required by Education's Student Financial Aid Handbook.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

May 26, 2023

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
The College of William and Mary in Virginia

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

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of **The College of William and Mary in Virginia** (the University) as of and for the year ended June 30, 2022, and the related notes to the financial statements, which collectively comprise the University's consolidated basic financial statements and have issued our report thereon dated May 26, 2023. 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.

Internal Control Over Financial Reporting

In planning and performing our audit of the consolidated 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 consolidated 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 Firewall Security," "Develop and Implement a Service Provider Oversight Process," "Improve Database Security," "Improve IT Risk Management Program," "Improve Controls over Contract Administration and Management," and "Improve Federal Financial Aid Reconciliation Controls," 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 consolidated 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 Firewall Security," "Develop and Implement a Service Provider Oversight Process," "Improve Database Security," "Improve IT Risk Management Program," and "Improve Federal Financial Aid Reconciliation Controls."

The University's Response to Findings

We discussed this report with management at an exit conference held on May 12, 2023. 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 "Richard Bland Response." Richard Bland's response was not subjected to the other auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

William & Mary has taken adequate corrective action with respect to audit findings reported in the prior year. Richard Bland has not taken adequate corrective action with respect to the previously reported findings, currently titled "Improve Firewall Security" and "Develop and Implement a Service Provider Oversight Process." Accordingly, we included these findings in the section titled "Internal Control and Compliance Findings and Recommendations." Richard Bland 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

EMS/vks

Richard Bland College
of WILLIAM & MARY

Office of Finance

June 27, 2023

Ms. Staci A. Henshaw, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218-1295

Dear Ms. Henshaw:

Richard Bland College has reviewed the Internal Control and Compliance Findings and Recommendations provided by the Auditor of Public Accounts for the fiscal year ended June 30, 2022. I hereby provide the following response for inclusion in the audit report:

Improve Firewall Security
Management concurs with the auditor's finding and Richard Bland continues to implement corrective action to address the concerns.

Develop and Implement a Service Provider Oversight Process
Management concurs with the auditor's finding. Richard Bland College is committed to developing and employing effective service provider oversight in alignment with applicable state policies and has taken measures to improve the current process.

Improve Banner Oracle Database Security
Management concurs with the auditor's finding and Richard Bland will implement corrective action to address the concerns.

Improve IT Risk Management Program
Management concurs with the auditor's finding and Richard Bland will implement corrective action to address the concerns.

Improve Controls over Contract Administration and Management
Management concurs with the auditor's finding and Richard Bland will implement corrective action to comply with state policies and has taken measures to improve the current process.

Improve Federal Financial Aid Reconciliation Controls
Management concurs with the auditor's finding. Richard Bland has updated its policies and procedures to ensure timely, accurate, and complete reconciliation of and the disbursement of federal financial assistance programs.

11301 Johnson Road, South Prince George, Virginia 23805
804-862-6100 | RBC.edu

Richard Bland College
of WILLIAM & MARY

Office of Finance

Please contact me should you have any questions.

Sincerely,

Stacey A. Sokol
Chief Business Officer

11301 Johnson Road, South Prince George, Virginia 23805
804-862-6100|RBC.edu

THE COLLEGE OF WILLIAM & MARY IN VIRGINIA
RICHARD BLAND COLLEGE

As of June 30, 2022

BOARD OF VISITORS

John E. Littel, Rector
William H. Payne, II, Vice Rector
Barbara L. Johnson, Secretary

Mari Carmen Aponte
Victor K. Branch
S. Douglas Bunch
Sue H. Gerdelman
James A. Hixon
Cynthia E. Hudson
Anne Leigh Kerr
Charles E. Poston
John P. Rathbone
Lisa E. Roday
J.E. Lincoln Saunders
Karen Kennedy Schultz
Ardine Williams
Brian P. Woolfolk

ADMINISTRATIVE OFFICIALS

The College of William and Mary in Virginia

Katherine A. Rowe, President

Amy S. Sebring, Chief Operating Officer

Richard Bland College

Debbie L. Sydow, President