THE COLLEGE OF WILLIAM AND MARY IN VIRGINIA

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2013

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of the College of William and Mary, including the Virginia Institute of Marine Science and Richard Bland College, as of and for the year ended June 30, 2013, and issued our report thereon, dated May 16, 2014. Our report, included in the College's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the College's website at www.wm.edu.

Our audit of the College of William and Mary for the year ended June 30, 2013, found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring the attention of management at both the College of William and Mary and Richard Bland College; 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.

The College has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

–TABLE OF CONTENTS–

AUDIT FINDINGS AND RECOMMENDATIONS – THE COLLEGE OF WILLIAM AND MARY

Improve the Vendor Payment Process

The College of William and Mary's (College) accounts payable department did not process vendor payments in accordance with the Commonwealth's Accounting Policies and Procedures (CAPP) Manual nor the Virginia Public Procurement Act. Although the College has been granted the autonomy to develop its own policies and procedures as a Tier III Institution, the College has elected to employ and abide by the Commonwealth's policies in this regard. Hence, in applying those policies, our review of expenditure vouchers found two processed without supporting documentation, three processed with no evidence of approval, and four processed more than 30 days after receipt of the vendor invoice.

According to CAPP Manual Topic 20310, the original vendor prepared bill must be attached to the payment as supporting documentation. The policy further states that the authorization, recordation, and control disbursement of transactions is mandatory. Additionally, §2.2-4347 of the Virginia Public Procurement Act requires payment for delivered goods and services within 30 calendar days after receipt of a proper invoice or 30 days after receipt of the goods or services, whichever is later.

Recommendation

We recommend the College enhance and enforce existing internal controls surrounding the disbursement process to ensure proper compliance with the CAPP Manual and the Virginia Public Procurement Act. Without adequate adherence and enforcement of these policies, the College is exposed to the risk of improper payments being processed.

Improve the Termination Process

The College should improve the process of identifying and reporting terminated employees to the Offices of Human Resources and Student Financial Aid. Our review found six instances where faculty and student workers did not have the proper forms submitted to the required offices upon their termination. The College's Administrative Policy and Procedures Manual requires the timely submission of these forms to ensure all property of the College is returned prior to providing final payment of services. Adherence to this policy is a necessary component for the College to have assurance that all property is being properly surrendered upon an employee's termination and that all levels of system access are being timely removed.

Recommendation

We recommend the College enforce and strengthen its existing policy regarding the timely submission of required forms upon the notification of an employee's termination. The College

should also strive to ensure all required notifications of termination are maintained within the employee's human resource file to reduce the risk of improper payment and to provide assurance of all College property being returned upon an employee's termination.

Improve eVA Internal Controls and Compliance

The College did not comply with several requirements contained in the eVA Electronic Procurement System Security Standards (Security Standards) issued by the Department of General Services (DGS) related to internal controls and the proper monitoring of access surrounding the use of eVA. Our review identified several instances of improper and untimely deactivation of eVA access. We also found the College does not have an eVA Security Plan in place nor a policy detailing allowable "on-behalf" purchases made by individuals other than the designated purchase charge card holder. Further details related to the items referenced above and the governing sections of the Security Standards are included below.

- The Procurement Officer, who serves as the Administrative Head of the Procurement Department, was designated as one of three eVA Security Officers. As the eVA Security Officer role allows for the setting up and removal of users in eVA, Section 1.1 through 1.3 of the Security Standards indicates that only a primary and a backup should be designated as a security officer and neither should be a procurement or fiscal officer with any level of financial exposure.

- An Associate Director of Procurement was granted access to the administration application in eVA, which allows for the management of all eVA users of the College. According to Section 2.4 of the Security Standards, this level of access should only be granted to eVA Security Officers.

- Two terminated employees of the College were not de-activated from eVA in a timely manner. According to Section 2.8 of the Security Standards, terminated employees should be immediately reported to the Security Officer to ensure access to the system is deleted.

- An eVA user access review was performed by the College during the year; however, it did not identify users whom have never logged into the system. Section 2.8 of the Security Standards requires that access reviews include the review of all inactive users to identify individuals whom no longer need access.

- The College did not have an Entity eVA Security Plan in place as required by Section 1.3.1 of the Security Standard.

- Lastly, we found the College allows the Virginia Institute of Marine Science (VIMS) employees to make purchases through eVA on behalf of other employees whom actually hold purchase charge cards. While this is an allowable practice, the College's

Small Purchase Charge Card Policy currently does not describe the process by which this should be done per guidelines included within the Security Standards.

Recommendation

We recommend the College improve the process by which eVA access is managed and monitored, ensuring eVA users are being granted access based on the principle of least privilege as prescribed by the Security Standards. By doing so, the risk of improper purchases will be lowered and the overall controls surrounding the procurement cycle will be improved. The College should also revise its policy on the use of small purchase charge cards to indicate when card information can be shared and how this activity should be monitored.

Improve System Security Reviews

The College does not perform adequate user access reviews of sensitive functions in the Banner System. To manage Banner access, the College establishes user classes, which generally relate to a specific job function and identifies the Banner screens the user can view and change. By allowing inappropriate access to certain screens in Banner, the College cannot assure the proper separation of duties exist within the system. During our review, we found numerous instances of inappropriate end users access levels within the system, which increases the risk of inadequate internal controls surrounding the use of Banner.

Recommendation

We recommend the College improve the process by which access reviews to sensitive functions in Banner are performed to ensure access is granted and maintained on the principle of least privilege. At a minimum, the College should annually perform an evaluation of access to sensitive functions to ensure adequate separation of duties exists. Further, when an access review is performed, department managers should provide justification for any employee that has access to functions deemed sensitive in nature that do not reasonably relate to their current job functions. By including the consideration of sensitive functions and forms within the Banner System access review, the College's overall risk of improper access and processing of financial data will decrease.

AUDIT FINDINGS AND RECOMMENDATIONS – RICHARD BLAND COLLEGE

Improve Information Security Program

Richard Bland College (RBC) does not have an information security program that provides the necessary requirements, guidance, and controls to secure its mission critical systems and sensitive data. The weaknesses identified significantly weaken the controls protecting the sensitive and mission critical systems and data at RBC.

Our review of RBC's information security program against the Commonwealth Information Security Standard, SEC 501-07.1 identified the following weaknesses:

- No formal IT change control management process or system is implemented for Banner hardware and software changes. Establishing a change control management process and system will reduce the risk of a change negatively impacting RBC. *(SEC 501-07.1: CM-9 Configuration Management)*.

- Password requirements are not enforced as required by RBC policy. Strong passwords reduce the risk of a compromised user account. *(SEC 501-07.1: IA-5 Authenticator Management)*.

- Security awareness training is not provided to all employees as required by RBC policy. Approximately 76 percent of staff did not complete annual security awareness training in fiscal year 2013. Providing annual training and security education to employees reduces the risk of an employee making costly errors in regard to information security. *(SEC 501-07.1: AT-2 Security Awareness)*.

- Backups are not stored off-site. Secure off-site storage reduces the risk of RBC losing its critical information in the event of a disaster. *(SEC 501-07.1: CP-9-COV Information System Backup)*.

- Roles and responsibilities specific for the Information Security Officer (ISO) are not established. Further, the ISO is not independent of the Chief Information Officer (CIO). Segregation of duties reduces the conflict of interest between the person implementing security (CIO) and the person reviewing security compliance and controls (ISO). *(SEC 501-07.1: 2.5 Information Security Officer)*.

- An up-to-date risk assessment is not documented. A risk assessment will help RBC identify potential threats for its mission critical and sensitive systems. *(SEC 501-07.1: 6 Risk Assessment)*.

- Recovery Point Objectives (RPOs) are not defined. Assessing and defining RPOs will help RBC ensure complete data recovery for its mission critical systems in the event

of a disaster or incident that negatively affects RBC's mission critical and sensitive systems. *(SEC 501-07.1: 3.2 Business Impact Analysis)*.

- Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP) tests are not performed. Further, DRP team members do not receive position-specific training. Annually testing the COOP and DRP, along with training the team members, will help RBC ensure its preparedness for a disaster or incident negatively affecting RBC. *(SEC 501-07.1: CP-4 Contingency Plan Testing and Exercises).*

Recommendation

We recognize that RBC's IT management is new and is committed to strengthening RBC's information security program moving forward. We recommend that RBC dedicate the necessary resources to assess and implement the controls outlined above in accordance with SEC501-07.1 and industry best practices to help strengthen RBC's security posture.

Improve Web Application Security

RBC lacks certain controls for its publicly facing web application that handles sensitive information for its mission critical ERP system, Banner. The Commonwealth's Information Security Standard, SEC 501-7.1, requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

We identified and communicated two weaknesses to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

May 16, 2014

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable John C. Watkins
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
The College of William and Mary

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**, including the Virginia Institute of Marine Science and Richard Bland College (the College), as of and for the year ended June 30, 2013, and the related notes to the financial statements, which collectively comprise the College's basic financial statements and have issued our report thereon dated May 16, 2014. 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 College, 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 College's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the College's internal control over

financial reporting. Accordingly, we do not express an opinion on the effectiveness of the College's internal control over financial reporting.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified. We did identify certain deficiencies in internal control over financial reporting entitled "Improve Vendor Payment Process," "Improve the Termination Process," "Improve eVA Internal Controls and Compliance," "Improve System Security Reviews," "Improve Information Security Program," and "Improve Web Application Reviews," which are described in the sections titled "Audit Findings and Recommendations – The College of William and Mary" and "Audit Findings and Recommendations – Richard Bland College" that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the College's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the sections titled "Audit Findings and Recommendations – The College of William and Mary" and "Audit Findings and Recommendations – Richard Bland College" in the findings entitled "Improve Vendor Payment Process," "Improve eVA Internal Controls and Compliance," "Improve Information Security Program," and "Improve Web Application Reviews."

Response to Findings

We discussed this report with management at exit conferences held on May 28, 2014. The College's and Richard Bland College's responses to the findings identified in our audit are described in the accompanying section titled "Agency Response." The responses were 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 College has taken adequate corrective action with respect to audit findings reported in the prior year.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

AUDITOR OF PUBLIC ACCOUNTS

BDH/alh

CHARTERED 1693

THE COLLEGE OF WILLIAM AND MARY IN VIRGINIA
OFFICE OF FINANCE
POST OFFICE BOX 8795
WILLIAMSBURG, VIRGINIA 23187-8795

757/221-2740, FAX 757/221-2749

May 23, 2014

Ms. Martha Mavredes
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Mavredes:

In response to the College's fiscal year 2013 audit findings and recommendations, I hereby provide the following responses for inclusion in the audit report.

- Improve the Vendor Payment Process.

  Management agrees with the auditor's finding and has reviewed them with the appropriate mangers and staff. The College's comptroller will continue to enhance our quality assurance review of vendor payments to ensure compliance with disbursement policy.

- Improve the Termination Process.

  Management agrees with the auditor's finding and has enacted various actions to resolve the concerns including a reminder from the provost to the campus of the importance adhering to the termination policy, the human resource staff meeting with academic and administrative departments to reinforce the policy's requirements and procedures, and revisions to the policy and procedures for improve enforcement. The College's associate vice president for human resources will be responsible for enacting these changes.

- Improve eVA Internal Controls and Compliance

  Management agrees with the auditor's findings. The director of procurement is responsible for responding to the auditor's concerns has immediately corrected certain items and is researching alternatives to correct the other items.

- Improve System Security Reviews.

  Management agrees with the auditor's finding and had already implemented changes and has plans in place for this summer's annual review to address the auditor's concerns. The College's director of information security and project management will continue to enhance the security access reviews as recommended.

Please contact me should you have any questions.

Sincerely,

Samuel E. Jones
Vice President for Finance

May 19, 2014

Please accept this as Richard Bland College's formal response, requested to be completed and returned by Tuesday, May 20, 2014. We submit this ahead of our exit conference, which is scheduled for May 28th, 2014.

Richard Bland College acknowledges receipt of the APA's audit findings and recommendations in regards to the fiscal year ended June 30, 2013. We understand this is the first fiscal year that a more clear distinction was made by the APA between The College of William and Mary and Richard Bland College. This new, greater distinction between the two state agencies resulted in an expanded audit scope from prior fiscal periods. As a result of this change in assigned audit scope, we are issuing our own Collegiate response, separate from the response from The College of William and Mary.

We have reviewed your findings and recommendations in full. We appreciate your thoroughness, diligence, timeliness, and effectiveness in all regards for the fiscal year 2013 audit.

Please refer to the College Corrective Action Plan, as communicated to the APA on April 10th, 2014, for intended correction of weaknesses identified in our information security programs. This communication conveys specific plans including an anticipated timeline.

We understand that you do not express an opinion on the effectiveness of the College's internal control over financial reporting. We consider the adequacy of internal controls in all policies and procedures at the College. We feel strongly about the adequacy of existing internal controls. We acknowledge the possibility exists for some improvement in internal controls but are, at times, limited by resource availability.

THE COLLEGE OF WILLIAM AND MARY IN VIRGINIA

BOARD OF VISITORS

Jeffrey B. Trammell – Rector

Charles A. Banks III - Vice Rector

Dennis H. Liberson - Secretary

Kendrick F. Ashton, Jr.
Ann Green Baise
Keith S. Fimian
Edward L. Flippen
Thomas R. Frantz
Sue H. Gerdelman
John E. Littel
Leigh A. Pence
L. Clifford Schroeder, Sr.
Robert E. Scott
Peter A. Snyder
Todd A. Stottlemyer
Michael Tang
John Charles Thomas

Curtis A. Mills, Student Representative
William J. Hausman, Faculty Representative
Jessica C. Salazar, Student Representative
Barbara M. Morgan, Faculty Representative

COLLEGE OFFICIALS

THE COLLEGE OF WILLIAM AND MARY IN VIRGINIA

W. Taylor Reveley III, President
Michael R. Halleran, Provost
Virginia M. Ambler, Vice President for Student Affairs
James R. Golden, Vice President for Strategic Initiatives
Samuel E. Jones, Vice President for Finance
Anna B. Martin, Vice President for Administration
Matthew T. Lambert, Vice President for Development

RICHARD BLAND COLLEGE

Debbie L. Sydow, President
LeAnn Binger, Provost and Dean of Faculty
Annette Parker, Vice President of Administration and Finance