



THE COLLEGE OF WILLIAM AND MARY
IN VIRGINIA
VIRGINIA INSTITUTE OF MARINE SCIENCE
AND
RICHARD BLAND COLLEGE

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2016

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 in Virginia, including the Virginia Institute of Marine Science and Richard Bland College (the Colleges), as of and for the year ended June 30, 2016, and issued our report thereon, dated September 8, 2017. Our report, included in the Colleges' basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the College of William and Mary's website at www.wm.edu.

Our audit of the Colleges, for the year ended June 30, 2016, found:

- the financial statements are presented fairly, in all material respects;
- deficiencies which we consider to be material weaknesses in internal control over financial reporting and information security at Richard Bland College;
- additional internal control findings at the Colleges requiring management's attention; however, we do not consider them to be material weaknesses; and
- instances of noncompliance or other matters at the Colleges required to be reported under Government Auditing Standards.

– TABLE OF CONTENTS –

| | <u>Pages</u> |
|--|--------------|
| AUDIT SUMMARY | |
| STATUS OF PRIOR YEAR FINDINGS - THE COLLEGE OF WILLIAM AND MARY | 1-2 |
| AUDIT FINDINGS AND RECOMMENDATIONS – THE COLLEGE OF WILLIAM AND MARY | 3-4 |
| STATUS OF PRIOR YEAR FINDINGS – RICHARD BLAND COLLEGE | 5-9 |
| AUDIT FINDINGS AND RECOMMENDATIONS – RICHARD BLAND COLLEGE | 10-14 |
| INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS | 15-18 |
| THE COLLEGE OF WILLIAM AND MARY RESPONSE | 19-20 |
| RICHARD BLAND COLLEGE RESPONSE | 21-24 |
| COLLEGE OFFICIALS | 25 |

STATUS OF PRIOR YEAR FINDINGS – THE COLLEGE OF WILLIAM AND MARY

Improve the Employee Termination Process

Type: Internal Control

Severity: Significant Deficiency

Repeat: Yes

During the fiscal year 2014 audit, we recommended that the College of William and Mary (William and Mary) improve the employee termination process. Departments were not completing the employee termination checklist, which the College's Human Resources Policy requires. During the fiscal year 2015 audit, the Office of Human Resources was still in the process of implementing its full corrective action plan. During this year's audit, we tested the termination checklist process and were unable to obtain the clearance forms required by the Employee Clearance Policy (the Policy) for six of 18 employees sampled (33 percent). As a result, William and Mary could not prove it collected certain items such as charge cards, keys, IDs, or fines owed prior to the employee's last day on campus, nor could William and Mary support the date of termination reporting in the financial accounting and reporting system. Additionally, William and Mary was not aware that it had not paid the necessary leave payout due to one employee.

According to the Policy, an employee should obtain a clearance form from the Office of Human Resources website. The employee is responsible for obtaining the appropriate departmental signatures or clearance e-mails from the listed departments and submitting the completed clearance form to the Office of Human Resources prior to his or her departure. The Policy further states that William and Mary will release the final paycheck and/or leave payoff check to the employee once the employee completes the clearance process. As part of this process, Human Resources runs a report each pay period that identifies terminated employees with leave balances. Human Resources sends this report to the Payroll Department for payment of leave balances owed.

By issuing paychecks prior to the collection of the completed clearance forms, William and Mary eliminated the main mechanism established by the Policy to encourage the submission of the clearance forms. Regarding the missed leave payout, the Human Resources report that is run each pay period did not include this employee because his Personnel Action Form was received late (after the pay period) by Human Resources. When employees do not complete the clearance form, there is an increased risk of paying employees after termination or allowing employees to retain access to important information systems. Additionally, William and Mary may not properly collect college property such as keys, credit cards, or fines owed prior to the employee's final day of employment. Finally, the Human Resources Department may not identify and pay amounts owed to terminated employees for accumulated leave balances.

William and Mary should enforce the Employee Clearance Policy to obtain required clearance forms from terminating employees before releasing the employee's final paycheck or leave payout. Following the Employee Clearance Policy will reduce the risk of improper payments to terminated employees, ensure timely termination of access to College or State systems, and provide for proper collection of College property.

Improve Database Security Controls

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Partial with limited progress

Prior Title: Improve Database Security

William and Mary does not implement some of the required logging and monitoring controls to protect the database that supports the financial accounting and reporting system in accordance with their adopted information security standard, ISO 27002 (Security Standard). The Security Standard requires the implementation of adequate security controls to safeguard systems that contain or process sensitive and financial data.

We communicated the details of the weaknesses to management in a separate document marked Freedom of Information Act Exempt under Code of Virginia §2.2-3705.2, due to their sensitivity and description of security controls.

The College did not resolve the prior year finding due to its interpretation of the importance of the required controls. The College should dedicate the necessary resources to improve database monitoring controls to further reduce risk and provide stronger security for the database that supports the financial management system.

Improve Controls over Timesheet Approval

Type: Internal Control

Severity: Significant Deficiency

Repeat: Partial with significant progress

During the fiscal year 2014 and 2015 audits, we identified instances where the Payroll Department of William and Mary administratively approved timesheets that department supervisors did not approve by the required payroll deadline. During the fiscal year 2015 audit, we noted that the Payroll and the Information Technology Departments were coordinating to develop a process to identify supervisors who missed the deadline for approving timesheets. Once identified, Payroll planned to require positive confirmation from supervisors that employees charged the correct number of hours.

In May 2016, William and Mary implemented a new Administratively Approved Timesheet Policy (the Policy). Following the implementation of the Policy, supervisors must respond to payroll notifications by certifying that the time reported for each employee is correct within seven days of receiving the notification. If Payroll does not receive a response within seven days, it will follow up with the departmental approver's supervisor. Based on the current year's audit, Payroll continued to approve timesheets administratively through April 2016; however, following the implementation of the new policy, Payroll properly obtained confirmation from departmental approvers rather than continuing to administratively approve those timesheets. As a result, we consider this finding resolved as of May 2016. We will perform additional follow up testing during the fiscal year 2017 audit to confirm the corrective action remains effective.

AUDIT FINDINGS AND RECOMMENDATIONS – THE COLLEGE OF WILLIAM AND MARY

Improve Information Technology Change Control

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

William and Mary does not have an information technology (IT) change management program that meets the minimum requirements defined in the College's adopted information security standard, ISO 27002 (Security Standard).

We communicated the details of the control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Code of Virginia §2.2-3705.2, due to their sensitivity and description of security controls. In general, William and Mary lacks an adequate change control policy and a consistent process for documenting, maintaining, and searching change documentation.

IT department management should develop and implement a change control policy, with supporting procedures, to improve the change control program. At a minimum, management should consider including the recommended elements communicated in the FOIAE document. By implementing sufficient IT change controls, management will reduce the risk of unauthorized changes and will help improve the security and availability of mission critical and sensitive systems.

Improve Timeliness of Small Purchase Charge Card Reconciliations

Type: Internal Control

Severity: Significant Deficiency

Repeat: No

William and Mary should improve monitoring controls over its Small Purchase Charge Card (SPCC) program. Seven out of 20 reconciliations reviewed (35 percent) contained transactions which had not been reviewed and approved by the 23rd day of the month in which the cycle closed, in accordance with William and Mary SPCC Policies and Procedures. The length of time that transactions remained unapproved by either the cardholder or approver ranged from 14 to 147 days following the 23rd day of the month. While the SPCC Policies and Procedures state that accounts that remain unreconciled 60 days after the cycle deadline may be suspended, such suspension does not appear to be taking place. Three of the seven cardholders (42 percent) with transactions that remained unapproved for longer than 60 days continued to make purchases after 60 days and before the approval of the unreconciled transactions.

The Management Agreement By and Between the Commonwealth of Virginia and the College of William and Mary in Virginia (2006) directs William and Mary to create its own policies for managing disbursements, including those made by charge card. The William and Mary SPCC Policies and Procedures state it is the responsibility of the cardholder's authorized approver to review and approve all cardholder monthly statement reconciliations to ensure transactions are within policy and

appropriate. Additionally, SPCC cardholders and approvers are responsible for ensuring that monthly reconciliations are complete by the 23rd day of the month in which the cycle closes. Per William and Mary's SPCC Policies, failure to sign off on transactions by the cardholder or approver is a violation of the policy. The policy states that individuals who violate the SPCC procedures may have card privileges suspended or permanently revoked. Additionally, the policy withholds funds from the cardholders spending limit until unapproved transactions have been through the appropriate review and approval process.

Not properly monitoring and reconciling SPCC activity increases the risk of fraudulent or inappropriate purchases. As William and Mary, including the Virginia Institute of Marine Science, had 313 cardholders and combined expenditures of more than \$23 million during fiscal year 2016, delayed reconciliation of transactions increases the risk that cardholders may not detect fraudulent activity by external parties in a reasonable timeframe.

William and Mary should establish an adequate monthly process to monitor transactions that remain unapproved by either cardholder or approver after the 23rd day of the month in which the cycle closes. This monitoring process could include the Program Administrator following up with approvers who have unreconciled transactions or transactions lacking support. William and Mary may also want to consider tracking violations of the SPCC Policies and Procedures and implement additional consequences for individuals that do not comply.

STATUS OF PRIOR YEAR FINDINGS – RICHARD BLAND COLLEGE

Improve Controls over Financial Reporting

Type: Internal Control

Severity: Material Weakness

Repeat: Yes

Richard Bland College (Richard Bland) does not have adequate internal controls over its financial reporting process. Similar to previous years, numerous adjustments and errors to the financial statements indicate that the current process for compiling the financial statements does not prevent, or detect and correct on a timely basis, material misstatements to the financial statements.

During our review of financial information submitted by Richard Bland to William and Mary for consolidation in the combined financial statements, we found:

- Richard Bland made six adjustments to Beginning Net Position to correct errors in the prior year financial statement's ending net position. In one instance, Richard Bland incorrectly adjusted the Beginning Net position balance by \$331,047. Additionally, due to the method of compiling the financial statements from various sources, Richard Bland used a \$599,208 "plug" entry to Beginning Net Position to ensure agreement of the Net Position balances reported in the Statement of Net Position and the Statement of Revenues, Expenses, and Changes in Net Position.
- Richard Bland does not use a fixed asset tracking system. All fixed assets are tracked using spreadsheets. As a result of poor tracking during previous fiscal years, the capital asset footnote information reported to William and Mary contained "plug" numbers to calculate the correct ending balances. Due to previous lapses in internal control, Richard Bland was unable to identify the year it disposed of certain assets.
- Richard Bland mistakenly included \$2.7 million of Federal Direct Loans in its financial statements as a revenue and expense, even though the institution is only a pass-through entity for the funds and should not record the activity in its financial statements.
- Richard Bland understated operating expenses by \$2.1 million due to an insufficient understanding of the process for extracting its expenses from the Commonwealth's accounting and financial reporting system.
- Richard Bland did not reclassify the auxiliary fee, which Richard Bland includes with tuition in its accounting and financial reporting system when it charges students at the beginning of each semester, to the appropriate line item for financial reporting purposes. As Richard Bland compiled the financial statements without using its accounting and financial reporting system, it should have manually reclassified the auxiliary fee portion of \$1.1 million to the Auxiliary Enterprises line item, but the institution did not complete this reclassification.

- Richard Bland did not prorate an interest payment due in fiscal year 2017 between fiscal year 2016 and fiscal year 2017, causing a \$318,770 overstatement of Accrued Interest Payable. Additionally, Richard Bland understated Interest Expense on Capital Asset Related Debt by \$528,294 due to a misclassification of interest payments as auxiliary enterprise expenses.
- No verifiable support could be provided by Richard Bland to substantiate certain receivables due from the federal government. Richard Bland subsequently determined that \$500,674 originally reported as accounts receivable did not represent amounts due to Richard Bland as of June 30, 2016, and should be removed from the financial statements.
- Richard Bland did not report an allowance for doubtful accounts to reduce accounts receivable to its net realizable value. After further analysis, and as a result of an audit recommendation, Richard Bland reduced Student Accounts Receivable and Beginning Net Position by \$245,069 due to expected uncollectability.

Management is responsible for designing and maintaining a system of internal controls relevant to the preparation and fair presentation of financial statements that are free from material misstatement in accordance with generally accepted accounting principles. A lack of formalized procedures, significant personnel turnover in financial reporting and financial operations during the fiscal year, and an inability to rely on the institution's accounting and financial reporting system (resulting in the manual preparation of the trial balance from multiple sources) led to the issues identified. These weaknesses have increased the risk of misstatement and resulted in adjustments to both current and prior year financial statements. Inaccurate financial information can affect long-term planning and the decisions of those individuals or institutions that rely on such information.

As the prior year audit was not completed until fiscal year 2016 was over halfway complete, Richard Bland did not have sufficient time to completely address the recommendation from the prior year report. Since that time, Richard Bland has worked to improve staffing, document policies and procedures, and develop a system for financial reporting for fiscal year 2017. Richard Bland should continue to develop and implement policies and procedures over financial reporting, and should utilize its accounting and financial reporting system as the basis for producing its financial statements for fiscal year 2017. We will audit the institution's progress toward resolving the findings reported during the current and previous fiscal years during the fiscal year 2017 audit. As these changes occurred primarily at the end of fiscal year 2016, any expected impact should be noticeable during the fiscal year 2017 audit.

Comply with the Department of Human Resources Management Policy for Wage Employees

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes

Richard Bland College (Richard Bland) is not complying with the Department of Human Resource Management (DHRM) policy 2.20 (Policy) requiring non-benefit employees to work no more than 1500

hours during the May 1 to April 30 measurement period each year. Three non-benefit employees worked more than 1,500 hours from May 1, 2015, to April 30, 2016.

The Policy requires non-benefit employees to work no more than an average of 29 hours per week, for a maximum not to exceed 1,500 hours in the one-year measurement period of May 1 to April 30. DHRM developed this Policy to ensure that the Commonwealth is complying with the requirements of the Patient Protection and Affordable Care Act, which brings penalties for noncompliance.

Richard Bland currently has a notification process in place once an employee reaches 1,200 hours. The Department of Accounts' Payroll Service Bureau notifies Richard Bland once the employee reaches this threshold, and the Richard Bland Human Resource Department subsequently notifies the employee's supervisor. However, the existing process did not provide for continued monitoring of hours worked after the employee reached 1,200 hours.

To avoid penalty payments and ensure compliance with state and federal requirements, Richard Bland should refine its procedures to assist in monitoring non-benefit employees to ensure hours worked do not exceed 1,500 hours annually. As part of these procedures, Richard Bland may want to consider increasing the frequency of review of total hours worked and setting additional levels of notification to alert supervisors.

Improve Controls over Small Purchase Charge Cards

Type: Internal Control

Severity: Significant Deficiency

Repeat: Yes

Richard Bland College (Richard Bland) did not properly approve or review Small Purchase Charge Card (SPCC) transactions for 11 out of 25 (44 percent) transactions tested. Cardholders submitted documentation to the Bank of America Works (Works) website for these transactions, but there is no history or documentation of a supervisor approval. Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic No. 20355 (Purchase Charge Card) states that "procedures must ensure, at a minimum, that reconciled statements have been reviewed and approved in writing by the cardholder's supervisor or reviewer."

Not properly reviewing and approving SPCC cardholder reconciliations resulted from insufficient oversight by supervisors and the Purchase Card Administrator. When Richard Bland set up cardholders in Works, it did not implement system controls to ensure transactions automatically route to a supervisor for approval. The former Purchase Card Administrator allowed the issue to persist without correcting the system setup or implementing an alternative approval process. Additionally, supervisors did not approve all cardholder transactions for which they were responsible each month.

Insufficient review of purchase card transactions may result in untimely detection and correction of vendor overcharges, undetected cardholder misuse, or fraudulent purchases, which may result in financial loss to Richard Bland and the Commonwealth. The Purchase Card Administrator at Richard Bland should work with Bank of America and the Department of Accounts to set up the proper approval flow in Works for every cardholder, or the Purchase Card Administrator should implement a separate process to complete timely all required steps of cardholder reconciliation as described in the CAPP Manual.

Improve Controls over Expenditure Vouchers

Type: Internal Control

Severity: Significant Deficiency

Repeat: Yes

Richard Bland does not have adequate procedures in place for maintaining documentation supporting its expenditures. Richard Bland was unable to locate supporting expenditure documents for seven out of 22 (32 percent) items tested.

Topic 20310 of the CAPP Manual states, "Copies of expenditure documents are to be maintained on file at each agency for three years." Original documentation was not available due to misplacement of documentation during relocation of expenditure-supporting documents.

For the seven tested expenditures, Richard Bland could not verify that they paid the proper amount, properly approved payment, or properly coded the expenditure. Insufficient maintenance of supporting documentation increases the risk of improper payments to vendors or the possibility of fraud, and could potentially have an effect on Richard Bland's financial statements.

Richard Bland should ensure it establishes an organizational system that allows for proper maintenance and organization of expenditure documentation. When transporting files to a new storage location, Richard Bland should develop a process to account for all records.

Continue to Improve Information Security Program

Type: Internal Control and Compliance

Severity: Significant Deficiency*

Repeat: Yes

Richard Bland continues to lack an information security program that provides for all of the necessary requirements, guidance, and controls to secure its mission critical systems and sensitive data. Richard Bland continues to work to resolve four weaknesses in an effort to improve and mature the information security program and align it with the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard). Specifically, our review identified the following control areas that require continued improvement and resources.

IT Risk Management and Contingency Planning

- Richard Bland does not produce risk assessment executive summary reports for executive business leadership that include major findings and mitigation recommendations identified during the risk management process. A risk assessment executive summary is an essential control to establish the necessary communication between organizational business leadership and IT staff to work towards the mitigation of risks and hardening of mission critical IT systems (*Security Standard section: 6 Risk Assessment*).

*Information Security findings for Richard Bland are individually considered to be significant deficiencies, but collectively considered to be a material weakness.

- Richard Bland does not obtain documented executive level approval on its risk management and contingency planning artifacts. The Security Standard requires Richard Bland's President and Executive Staff's formal approval over the completed Business Impact Analysis, Risk Assessment(s), Continuity of Operations Plan, and Information Technology Disaster Recovery Plan to provide evidence of management's acknowledgement that these documents meet organizational needs for risk management and contingency planning efforts (*Security Standard section: 2 Agency Head*).

IT Security Awareness and Training

- Richard Bland does not provide security awareness training to all employees per its policy and the requirements of the Security Standard. Approximately 19 percent of employees did not complete the required training during fiscal year 2016. Providing annual training and security education to employees reduces the risk of an employee making costly security errors that could lead to a data breach. Richard Bland has made progress since last year's audit and should continue to strive towards ensuring that all users who access Richard Bland's systems and sensitive data have completed training before, or as soon as practicable after, receiving access rights to the IT systems (*Security Standard section: AT-2 Security Awareness*).
- Richard Bland does not provide periodic specialized training for users who serve in system administration roles, i.e. system owner, data owner, and data custodian. The Security Standard requires specialized training for these users so they are fully aware and equipped to perform their assigned role-based functions. In addition to the training, Richard Bland must document that each user formally accepts the designated role and is aware of the responsibilities associated with the related role (*Security Standard section: 2 Information Security Roles and Responsibilities*).

Richard Bland was unable to resolve the weaknesses noted above during the period following the prior year's audit due to a limited number of IT and security staff and significant employee turnover during the fiscal year. Additionally, Richard Bland dedicated resources to other enterprise-wide priorities.

Richard Bland should continue to allocate the necessary resources to develop, align, and implement an information security program in accordance with organizational policies and the Security Standard, as well as fully remediating the weaknesses noted above.

AUDIT FINDINGS AND RECOMMENDATIONS – RICHARD BLAND COLLEGE

Improve System Patch Management

Type: Internal Control and Compliance

Severity: Significant Deficiency*

Repeat: No

Richard Bland does not have sufficient patch management controls for systems that support mission critical business processes. The Security Standard requires the implementation of several patch management related controls to protect the confidentiality, integrity, and availability of sensitive and financial data.

The Security Standard requires the identification, testing, and implementation of software patches within 90 days of release (*Security Standard section: SI-2 Flaw Remediation*). Richard Bland lacks a policy outlining patching requirements, such as required testing and patching windows, which likely contributed to the delay in patching and updating certain software. Running outdated or unpatched software increases the risk that malicious individuals may exploit known vulnerabilities, potentially leading to a breach of sensitive data, resulting in legal, financial, or reputational damages for Richard Bland.

We communicated the details of the specific systems and software lacking appropriate patch controls to Richard Bland in a separate document marked Freedom of Information Act Exempt (FOIAE) under Code of Virginia §2.2-3705.2, due to their sensitivity and description of security controls.

Richard Bland should create a policy that contains the requirements for system patching and dedicate the necessary resources to evaluate, test, and install relevant security patches for the systems identified in the FOIAE document. The policy should also require Richard Bland to identify, evaluate, test, and implement patches within 90 days of release. Improving system patch management will reduce data security risk and better protect the confidentiality, integrity, and availability of sensitive and critical data.

Improve System Logging and Monitoring

Type: Internal Control and Compliance

Severity: Significant Deficiency*

Repeat: No

Richard Bland does not implement the necessary activity logging and monitoring controls for certain systems that support critical applications, including its financial accounting and reporting system, to effectively detect and prevent anomalies in sensitive and critical data and to comply with the Security Standard. Without adequate logging and monitoring controls, Richard Bland may not identify suspicious activity in a timely manner or retain vital information required for a forensic investigation. Insufficient logging and monitoring controls are a result of limited availability of information technology personnel and improper separation of duties.

*Information Security findings for Richard Bland are individually considered to be significant deficiencies, but collectively considered to be a material weakness.

We communicated the details of the control weaknesses to Richard Bland in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls.

Richard Bland should dedicate the necessary resources to implement the logging and monitoring controls described in the FOIAE document. By implementing the security controls, Richard Bland will reduce risk and provide stronger security for the systems that support mission critical business processes.

Improve Database and Network Security

Type: Internal Control and Compliance

Severity: Significant Deficiency*

Repeat: No

Richard Bland does not have certain required database and network security controls for systems to comply with the Security Standard and industry best practices. The Security Standard and best practices define security controls to protect the confidentiality, integrity, and availability of data stored in databases and transmitted over a network. A contributing factor to these weaknesses is that Richard Bland is not aware of all the requirements in the Security Standard and guidance of industry best practices.

We communicated the details of the control weaknesses to Richard Bland in a separate document marked Freedom of Information Act Exempt (FOIAE) under Code of Virginia §2.2-3705.2, due to their sensitivity and description of security controls. In general, the weaknesses included the use of a default account, insecure system configuration, and inadequate authentication controls.

Richard Bland should mitigate the weaknesses communicated in the FOIAE document and become familiar with, at a minimum, all the requirements in the Security Standard. Additionally, Richard Bland should evaluate and verify that current system configurations meet the minimum security controls mandated by the Security Standard and aligned with industry best practices, starting with sensitive and mission critical systems. To perform this assessment and verification, Richard Bland may need to dedicate additional staff and funding to implement the needed controls. These controls will reduce the data security risk for sensitive and mission critical systems and promote a more secure information technology environment.

Improve the myVRS Navigator Reconciliation Process

Type: Internal Control

Severity: Significant Deficiency

Repeat: No

Richard Bland did not perform and document reconciliations between *myVRS* Navigator and the Commonwealth's human resource system during fiscal year 2016. CAPP Manual Topic No. 50410 (Virginia Retirement System and Optional Retirement Plans) states that employers are responsible for ensuring valid interface values are in *myVRS* Navigator prior to the confirmation of the contribution snapshot.

*Information Security findings for Richard Bland are individually considered to be significant deficiencies, but collectively considered to be a material weakness.

The Human Resources Department at Richard Bland experienced significant turnover during the fiscal year, specifically in the Director of Human Resources position. Additionally, at certain times during fiscal year 2016, the Human Resources Department included only one full-time employee. These low staffing levels resulted in prioritization of various responsibilities and required tasks and lapses in performing certain required activities, such as reconciliation of retirement contributions. Not reconciling *myVRS Navigator* data with Commonwealth's human resource system data prior to certifying the snapshot increases the risk that Richard Bland's retirement contributions will be inaccurate. As the Commonwealth's actuary relies on the data reported in *myVRS Navigator* for determining the net pension liability for each of the Commonwealth's agencies and institutions, any inaccurate data reported by agencies and institutions can affect the actuary's analysis and potentially Richard Bland's financial statements.

Richard Bland should reduce position vacancies within the Human Resource Department to ensure completion of required procedures, such as reconciliations between *myVRS Navigator* and Commonwealth's human resources system. Furthermore, Richard Bland should work with the Department of Accounts' Payroll Service Bureau to clear ongoing data discrepancies.

Improve Compliance with the Prompt Pay Provisions of the Procurement Act

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Richard Bland did not make payments timely in accordance with the Prompt Pay Provisions of the Procurement Act. The Prompt Pay Provisions, as described in the Code of Virginia §2.2-4347, state that payments should be made 30 days after the later of receipt of invoice or receipt of item, or as established by contract. In a randomly selected sample, Richard Bland paid seven out of the 36 expenditures (19 percent) outside of the Prompt Pay Provisions requirement of 30 days.

The exceptions noted during testing occurred during December 2015 and January 2016. At that time, the employees responsible for issuing payments of expenditures were new hires still learning Richard Bland's systems. Due to their lack of experience and knowledge of the accounting systems, as well as a lack of documented payment procedures, the employees filled out the request for payment information incorrectly and the accounting system rejected the payment without their knowledge. The employees did not become aware of the errors until after the 30-day period.

Not complying with the Prompt Pay Provisions can damage relationships with vendors and harm the Commonwealth's reputation, as well as result in penalties in the form of interest due to the vendor. Richard Bland should document procedures for essential processes, such as vendor payments, and increase management oversight of new employees.

Develop and Implement Personnel Action Forms

Type: Internal Control

Severity: Significant Deficiency

Repeat: No

The Human Resources Department at Richard Bland lacked documented policies and procedures during fiscal year 2016 and; therefore, did not require personnel action forms (PAFs), or similar documentation, to support employee salaries. For all 16 (100 percent) of the salaried employees selected, Richard Bland was unable to provide properly completed forms to support the employees' salaries.

CAPP Manual Topic No. 50300, *Establish/Maintain Employee Profile Information*, states in Topic 50305 that, "Documentation supporting the hiring of employees must be properly completed and authorized before processing." Prior to certification, agencies are required to review all information pertaining to new hires and ensure the correctness of the data entry. Additionally, Topic 50310 requires appropriate supporting documentation for rehires and for supporting changes in employee pay. All applicable forms used to establish the employee record or make a change to the current information should be maintained for audit purposes. Since Richard Bland uses the Department of Accounts' Payroll Service Bureau to process its payroll, it is important that the information Richard Bland enters into the human resource management system is accurate and supported by appropriate documentation. Without appropriate supporting documentation, there is a chance that an employee's payroll may be incorrect, but with no form of verification.

Richard Bland's Human Resources Department should continue to develop and implement policies and procedures, including requiring a form to track employee salary and pay changes along with the necessary approvals.

Improve the Employee Termination Process

Type: Internal Control

Severity: Significant Deficiency

Repeat: No

The Human Resources Department at Richard Bland lacked documented policies and procedures during fiscal year 2016 and; therefore, did not require documentation of the collection of its property from terminated employees. Due to the lack of documentation, the Human Resources Department is unable to confirm the collection of Richard Bland's property for all four (100 percent) employees selected for testing.

CAPP Manual Topic No. 50320, *Terminations*, states that agencies should "develop a termination check-off list to ensure that all information is complete and accurate before terminating the employee." The recommended checklist should provide confirmation of the collection of any access badges, keys, or other equipment assigned to the employee. The absence of a separation checklist increases the risk of

misappropriation of assets or potential security concerns with non-employees having the ability to access Richard Bland facilities.

Richard Bland's Human Resources Department should continue to develop and implement policies and procedures that require supervisors to complete a separation checklist upon an employee's termination. Furthermore, Human Resources should communicate the importance of properly completing the checklist to all Richard Bland Departments.

Develop Policies and Procedures to Identify Potential Capital Assets

Type: Internal Control

Severity: Significant Deficiency

Repeat: No

Richard Bland did not properly review equipment purchases in order to capitalize assets during fiscal year 2016. In a randomly selected sample of equipment purchases, two of the eight expenditures reviewed (25 percent) met Richard Bland's capitalization criteria, but the institution did not record these items as capital assets. Richard Bland did not report any equipment additions in its listing of capital assets for fiscal year 2016.

CAPP Manual, Topic No. 30305, *Capitalized or Controlled Assets*, states that, "Each agency and institution should implement cost beneficial internal control procedures to ensure that assets are properly classified for financial reporting purposes." Topic 30305 also states that an asset meets capitalization criteria if it "has an expected useful life of greater than one year and the asset individually has a value or cost of \$5,000 or more at the date of acquisition."

Richard Bland lacked a documented process in place during fiscal year 2016 to require a review of large purchases to identify potential capital assets. As such, Richard Bland did not sufficiently review large purchases for potential capitalization, leading to an overstatement of expenses and an understatement of assets in the institution's financial statements. In addition to the improper classification within the institution's financial statements, improper identification of fixed assets at the time of purchase can also result in improper tagging and tracking of the asset while it is in use, and could increase the risk of misappropriation of the asset.

Richard Bland should develop and implement policies and procedures to properly capitalize purchased equipment meeting its capitalization threshold, including identifying the individual responsible for making such determinations.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 8, 2017

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Robert D. Orrrock, Sr.
Chairman, 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**, including the **Virginia Institute of Marine Science** and **Richard Bland College** (the Colleges), as of and for the year ended June 30, 2016, and the related notes to the financial statements, which collectively comprise the Colleges' basic financial statements and have issued our report thereon dated September 8, 2017. 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 Colleges', 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 Colleges' internal control over financial reporting to determine the 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 Colleges' internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Colleges' internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph 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. However, as described in the sections entitled “Status of Prior Year Findings – The College of William and Mary,” “Audit Findings and Recommendations – The College of William and Mary,” “Status of Prior Year Findings – Richard Bland College,” and “Audit Findings and Recommendations – Richard Bland College,” we identified certain deficiencies in internal control over financial reporting that we consider to be material weaknesses and significant deficiencies.

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. We consider the deficiency entitled “Improve Controls over Financial Reporting”, which is described in the section titled “Status of Prior Year Findings – Richard Bland College” to be a material weakness, and the significant deficiencies entitled “Continue to Improve Information Security Program,” “Improve System Patch Management,” “Improve System Logging and Monitoring,” and “Improve Database and Network Security,” which are described in the sections entitled “Status of Prior Year Findings – Richard Bland College,” and “Audit Findings and Recommendations – Richard Bland College” to collectively be a material weakness.

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. We consider the deficiencies entitled “Improve the Employee Termination Process,” “Improve Controls over Timesheet Approval,” and “Improve Database Security Controls”, which are described in the section titled “Status of Prior Year Findings – The College of William and Mary,” the deficiencies entitled “Improve Information Technology Change Control” and “Improve Timeliness of Small Purchase Charge Card Reconciliations,” which are described in the section titled “Audit Findings and Recommendations – The College of William and Mary,” the deficiencies entitled “Comply with the Department of Human Resources Management Policy for Wage Employees,” “Improve Controls over Small Purchase Charge Cards,” and “Improve Controls over Expenditure Vouchers,” which are described in the section titled “Status of Prior Year Findings – Richard Bland College,” and the deficiencies entitled “Improve the myVRS Navigator Reconciliation Process,” “Improve Compliance with the Prompt Pay Provisions of the Procurement Act,” “Develop and Implement Personnel Action Forms,” “Improve the Employee Termination Process,” and “Develop Policies and Procedures to Identify Potential Capital Assets” which are described in the section titled “Audit Findings and Recommendations – Richard Bland College” to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Colleges' financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the sections titled "Status of Prior Year Findings – The College of William and Mary," "Audit Findings and Recommendations – The College of William and Mary," "Status of Prior Year Findings – Richard Bland College," and "Audit Findings and Recommendations – Richard Bland College" in the findings entitled "Improve Database Security Controls," "Improve Information Technology Change Control," "Comply with the Department of Human Resources Management Policy for Wage Employees," "Continue to Improve Information Security Program," "Improve System Patch Management," "Improve System Logging and Monitoring," "Improve Database and Network Security," and "Improve Compliance with the Prompt Pay Provisions of the Procurement Act."

The Colleges' Responses to Findings

We discussed this report with management at an exit conference held on September 5, 2017. The Colleges' response to the findings identified in our audit is described in the accompanying sections titled "The College of William and Mary Response" and "Richard Bland College Response." The Colleges' response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings

The College of William and Mary has not taken adequate corrective action with respect to the previously reported finding "Improve the Employee Termination Process." The College of William and Mary has completed partial corrective action with respect to the previously reported findings "Improve Controls over Timesheet Approvals" and "Improve Database Security Controls." Accordingly, we included these findings in the section entitled "Status of Prior Year Findings – The College of William and Mary." Richard Bland College has not taken adequate corrective action with respect to the previously reported findings "Improve Controls over Financial Reporting," "Comply with the Department of Human Resources Management Policy for Wage Employees," "Improve Controls over Small Purchase Charge Cards," "Improve Controls over Expenditure Vouchers," and "Continue to Improve Information Security Program." Accordingly, we included these findings in the section entitled "Status of Prior Year Findings – Richard Bland College." The Colleges have taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Purpose of this Report

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

AUDITOR OF PUBLIC ACCOUNTS

EMS/alh



WILLIAM & MARY

CHARTERED 1693

OFFICE OF FINANCE AND ADMINISTRATION

September 8, 2017

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

Dear Ms. Mavredes:

After reviewing the College of William and Mary's fiscal year 2016 (FY16) audit findings and recommendations, I hereby provide the following responses for inclusion in the audit report:

- Improve the Employee Termination Process

Management agrees with the auditor's finding and Human Resources has implemented an electronic clearance form to replace the paper form that was used in the past. This electronic form will be completed by the department, as opposed to the employee and will be automatically routed to ensure more accurate and complete clearance records.

- Improve Database Security Controls

Management agrees with the auditor's finding and Information Technology has developed a remediation plan to address the required logging and monitoring controls to protect the database in accordance with ISO 27002 Information Security Standard.

- Improve Information Technology Change Control

Management agrees with the auditor's finding and Information Technology has developed a remediation plan to include a policy and supporting procedures to ensure compliance with ISO 27002 Information Security Standard.

- Improve Timeliness of Small Purchase Charge Card Reconciliations

Management agrees with the auditor's finding and Procurement Services has implemented a formal review process to identify any transactions that are not resolved within 60 days and to suspend accounts not reconciled after 60 days as stipulated in the policy.

Please note that Richard Bland College will be submitting a separate response.

P. O. Box 8795 • Williamsburg, VA 23187-8795 • (757) 221-2740

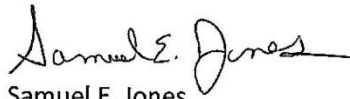
Ms. Martha S. Mavredes, CPA

-2-

September 8, 2017

Should you have any questions, please contact me.

Sincerely,

A handwritten signature in black ink that reads "Samuel E. Jones". The signature is fluid and cursive, with the first and last names being more prominent.

Samuel E. Jones

Senior Vice President for Finance and Administration

cc: Amy S. Sebring
Kent B. Erdahl
Courtney Carpenter
John M. Poma
Erma A. Baker
Melanie T. O'Dell



Richard Bland College of WILLIAM & MARY

Office of Finance

September 10, 2017

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

Dear Ms. Mavredes:

Richard Bland College of William and Mary has reviewed the Internal Control Findings and Recommendations provided by the Auditor of Public Accounts for fiscal year ending June 30, 2016 and is in agreement, in principle, with all of the findings submitted.

Attached for your consideration is an update as to where the campus is with respect to progress on these findings. The formal Corrective Action Workplan will be submitted within 30 days as required by CAPP Manual Section 10205. Please contact me if you have any additional questions or require additional information.

On behalf of Richard Bland College of William and Mary, please thank all of your staff for their professional work and recommendations to ensure RBC's continued success.

Sincerely,

Ms. Penelope G Howard
Chief Financial Officer

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

FY 2016 – Internal Control Findings and Recommendations

Human Resources

Develop and Implement Personnel Action Forms

As of June 30, 2017, the RBC Human Resources department has implemented various personnel action forms to include a Request to Recruit and a Request to Offer form, a Bonus Payment Request form, a Personnel Action Form, an Overload Payment Form, and a Special Payment Request Form. By October 31, 2017, the RBC Human Resources Department will have a page on the RBC website which will include all of these forms and instructions for use. HR will need to continue implementing personnel action forms to ensure proper approval and documentation of the many and various personnel actions.

Improve the Employee Termination Process

As of June 30, 2017, RBC Human Resources department has implemented a Separation Checklist. This checklist is now required for all employees who separate from RBC. It requires signature from the manager, the separating employee, and HR to affirm that all separation activities have been completed. The Separation Checklist will also be added to the RBC HR webpage to provide easy access for managers and an explanation of the process. HR will need to closely monitor and track completion of this checklist to ensure one is on file for every employee who separates employment.

Improve the myVRS Navigator Reconciliation Process

As of June 30, 2017, the RBC Human Resources department has improved the myVRS Navigator Reconciliation process by reducing the workload of the HR Specialist responsible for this task. In January 2017, a new HR Director was brought on board which allowed the HR Specialist to off-load responsibilities assumed while the HR Director position was vacant. The HR Analyst has also assumed more responsibility which gives the HR Specialist even more capacity to focus on the reconciliation process each month. We will need to ensure other members of the HR team are properly trained to complete monthly reconciliations to ensure someone is always able to complete them accurately and on a timely basis.

Information Technology

While we agree in principle with the information technology findings from the APA, we disagree with the APA auditor's conclusion that the four items identified in their report summarize to a material weakness. Major steps have been taken to mitigate the issues, with many solutions already complete in FY 17 prior to the audit review of the prior year, including the patch management and versioning finding, which was by far the most significant. We estimate that RBC is currently about 80-85% complete on upgrades and process development that resolve issues. The remaining items will take longer because we do not currently have the personnel or financial resources to implement solutions. The summary of progress on each finding is as follows:

Continue to Improve Information Security Programming

The Chief Information Officer is actively meeting with the Information & Technology Services (ITS) team weekly (sometimes daily when events occur) discussing risk and mitigation; the executive is highly involved and the executive team is regularly informed as we are all in the same hallway and meet continuously. Formalization of this process is time consuming and requires time that our Information Security Officer does not have as a single resource. We have put a number of reports in place, including a quarterly executive summary and will continue to add security reports as time and resources allows. Concerns about campus-wide security training is inflated as we went from < 20% of the campus trained in security awareness to 81% for the fiscal year in question, with most of the remaining employees in low technology areas such as food service and grounds. Additionally, there is extensive onboarding for

FY 2016 – Internal Control Findings and Recommendations

new employees and regular departmental security seminars taking place. The extensive amount of reporting required from Level I institutions by VITA is regularly accomplished and approved.

Improve System Patch Management

RBC corrected two of the three deficiencies immediately upon identification by the APA. We also acquired, back in 2016, a platform to support patching efforts across the campus and the vast majority of our systems are up to date. The primary system identified was on an unsupported version and has been upgraded after a year of work, work that was started several months before the APA identified this deficiency in its audit work.

Improve System Logging and Monitoring

While we understand what the APA is looking for, log monitoring at the level suggested is extremely time consuming and RBC simply does not have the resources to manage at this level, particularly when considering the cost/benefit payoff of implementing such a time intensive process. We are working with the General Assembly and William and Mary to staff a dedicated Network Engineer to take care of many other critical technology duties. This position may be able to put together a process that is scalable and address the underlying concern by the APA. As a mitigating factor, RBC does have several other active monitoring systems that help us identify and manage many of the risks the APA is concerned about.

Improve Database and Network Security

RBC immediately corrected one of the items identified by the APA upon notification, it was a best practice recommendation from the vendor and we actually chose to take the implementation a step further than required to ensure full implementation of the best practice. A second higher risk recommendation will require additional resources, both personnel and financial, but we will continue to work towards a solution in the meantime. While we understand the thoroughness with which the APA audits our systems, we do not fully believe several other minor items identified under this finding are a true risk as items that were present, but not active, were also identified and included in the recommendations. We will review these items again and implement as makes sense for RBC and we will implement a reporting process as suggested.

Finance

Improve Controls over Financial Reporting

Richard Bland College concurs with this finding and has worked diligently throughout fiscal years 2016, 2017, and into 2018 to address outstanding financial reporting issues.

Flawed financial reporting processes and reports are the result of a severely under-developed and under-resourced financial infrastructure. To address this longstanding vulnerability, management embarked on an aggressive re-set of the unit. During the spring of 2016 (FY 2016), the finance and financial aid modules of the accounting and financial reporting system were revitalized through appropriate updates, patches and the creation of a viable chart of accounts. These modules went live on July 1, 2016 (FY 2017) with a hard cutover that coincided with the beginning of a new academic year and the start of fiscal year 2016 financial statement preparation.

After multiple conversations with the APA in fiscal year 2016 and early fall of fiscal year 2017, the College proceeded to prepare a baseline set of auditable financial statements using the values on the Statement of Net Position (SNP) as the driving document for setting the baseline. The Statement of Net Position (SNP) consists of all the accounts that are both physical in nature (assets, cash, debt, etc.) and

FY 2016 – Internal Control Findings and Recommendations

are all independently verifiable through documents outside of the previous instance of the accounting and financial reporting system. After numerous conversations with the APA, this was chosen as the most reliable way to set the baseline financial position for RBC. Using this alternative methodology for building the financial statements did require multiple sources of account values, which as indicated in the audit finding, created some discrepancies on the Statement of Revenues, Expenses, and Net Position (SRECNP) as staff sought to make that document tie back to the SNP. It is important to note that prior to FY 2015, the College had never been audited as a stand-alone entity or on its financial statements independent of William and Mary's. During FY 2015, the BOV and William and Mary administration requested the APA perform RBC's financial statement audit independent of the William and Mary audit instead of continuing to audit its values in aggregate with William and Mary and VIMS as had historically been done. Due to this abrupt change in a decades' long process, and the subsequent turnover in financial staff at RBC in late FY 2015 and the first half of FY 2016, the preparation of the FY 2016 financial statements was destined to be difficult and time-consuming.

Despite the nearly complete turnover of financial staff in FY 2016 and the painstaking task of hiring and training new staff members, during the course of fiscal year 2017, RBC rebuilt financial processes, refined the new instance of the accounting and financial reporting system and the data being captured, and implemented a module specific for financial reporting. This newly built infrastructure has facilitated the development of FY 17 financial statements that leverage the accounting and financial reporting system.

The transformative work that has been accomplished by the Richard Bland College financial unit over the last 18 months enables the College to provide supported and auditable financial statements in a manner that has been recommended by both the APA and William and Mary for the past several years. The College anticipates this finding being fully addressed—or significantly reduced—with the audit of the FY 2017 financial statements.

The College does not leverage a fixed asset system outside of the excel spreadsheets. A cost benefit analysis done in FY 2016 did not find sufficient added value in implementing an electronic asset management system versus continuing a manual one for the small volume of assets procured each year. Processes are being improved to ensure better tracking of disposed assets, which has historically been the biggest issue with fixed assets management for RBC.

Improve Controls over Small Purchase Charge Cards Expenditure Vouchers, Improve Compliance with the Prompt Pay Provisions, and Develop Policies and Procedures to Identify Potential Capital Assets

RBC concurs with these additional important finance related findings. Significant progress has been made in these areas as well as part of the rebuild of the finance unit mentioned above during the course of FY 16, 17, and into FY 18.

**THE COLLEGE OF WILLIAM AND MARY IN VIRGINIA
RICHARD BLAND COLLEGE**

June 30, 2016

BOARD OF VISITORS

Todd A. Stottlemeyer – Rector
H. Thomas Watkins, III – Vice Rector
Sue H. Gerdelman – Secretary

| | |
|-------------------------|-----------------------|
| Kendrick F. Ashton, Jr. | Christopher M. Little |
| Ann Green Baise | William H. Payne, II |
| Lynn M. Dillon | Lisa E. Roday |
| Keith S. Fimian | Karen Kennedy Schultz |
| Thomas R. Frantz | Robert E. Scott |
| James A. Hixon | DeRonda M. Short |
| John E. Littel | John Charles Thomas |

Student Representatives

Yohance D. Whitaker – College of William and Mary
Amanda C. Archer – Richard Bland College

Faculty Representatives

Suzanne Raitt – College of William and Mary
D. Jill Mitten – Richard Bland College

Staff Liaison

Lyle M. Varnell – College of William and Mary

OFFICERS OF ADMINISTRATION

The College of William and Mary in Virginia

W. Taylor Reveley, III, President
Samuel E. Jones, Senior Vice President for Finance and Administration

Richard Bland College

Debbie L. Sydow, President
Penelope G. Howard, Dean of Finance and Administration