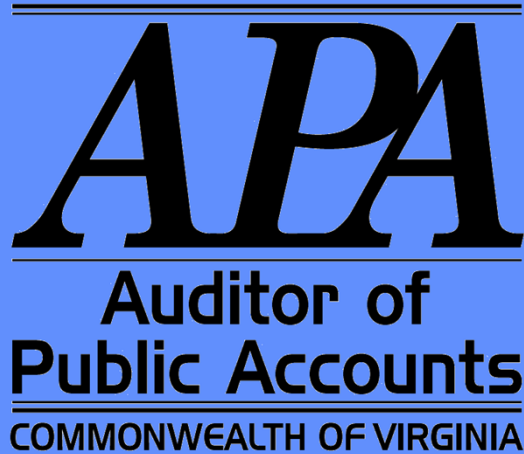


VIRGINIA STATE UNIVERSITY

**REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2010**



AUDIT SUMMARY

Our audit of Virginia State University for the year ended June 30, 2010, found:

- the financial statements are presented fairly, in all material respects, with generally accepted accounting principles;
- certain matters involving internal control findings requiring Management's attention; however, we do not consider them to be material weaknesses;
- instances of noncompliance or other matters required to be reported under Government Auditing Standards;
- the University has made progress, but has not completed corrective action with respect to the previously reported findings titled "Improve Database Management" and "Approve and Implement Updated Information Security Program", therefore, these findings are repeated in this year's report; and
- the University did take corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

We have audited the basic financial statements of Virginia State University as of and for the year ended June 30, 2010, and issued our report thereon, dated June 30, 2011. Our report, included in Virginia State University's Annual Financial Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at Virginia State University's website at www.vsu.edu.

–TABLE OF CONTENTS–

	<u>Pages</u>
AUDIT SUMMARY	
AUDIT FINDINGS AND RECOMMENDATIONS	1-2
INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	3-4
UNIVERSITY RESPONSE	5-6
UNIVERSITY OFFICIALS	7

AUDIT FINDINGS AND RECOMMENDATIONS

Improve Oracle Database Security

The University continues to incur the risk of a database failure or loss of data, because it has not implemented best practice controls to safeguard its mission critical and confidential data in its production databases. The University's inadequate controls create vulnerabilities that expose sensitive data and can possibly compromise data integrity.

Specifically, the University needs to improve password management, user profile setup, system auditing, and testing of backup and restoration procedures. We have communicated the details of these weaknesses to management in a separate document that is marked Freedom of Information Exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of a security system.

We recommend that the University complete its planned database upgrade and at the same time ensure compliance with industry best practices, University policies, and the Commonwealth's security standards. Further, the University should ensure that its technical staff is trained and aware of their newly established security requirements.

Approve and Implement Information Security Program

While the University has made progress towards implementing its information security program, this is the third report in a row that we have reported the need to completely and fully implement the Information Security Program. Typical universities of the size and complexity of Virginia State University review, update, and approve at least one-third of their entire information security program each year.

The University has not identified regulatory requirements, such as FERPA and PCI, for data types within their IT Data and System Classification document. Without identifying these regulatory requirements, the University cannot accurately identify which IT assets contain sensitive data. The University should complete and implement risk assessments as well as perform an annual self-assessment to determine the continued validity and need of each risk assessment.

Additionally, the University does not have manual procedures documented for essential business functions or sufficient disaster recovery procedures to guide the University's operations in case of a disaster that affects their information systems. Commonwealth recommended DRP appendixes are not included in the University's contingency planning documents.

We recommend that the University implement a self-assessment policy and process that reviews risk assessments for validity in accordance with the Commonwealth's information security standard. Further, we recommend the University amend the IT System and Data Sensitivity form to include a field to identify regulatory requirements specific to each data type.

Finally, the University should finalize, approve, and implement its information security program policies. We encourage the University to continue working diligently to complete the remaining incomplete sections of the information security program.

Strengthen Access Controls over eVA

During our review, we found the University's Security Officer did not request deletion of eVA access within one working day of employment termination for 5 of the 14 (36 percent) terminated employees tested, as required by the Security Manual. The delays in deleting access ranged from 24 days to over 19 months after the termination date.

Terminated employees with improper access to eVA could potentially enter and process false or fraudulent transactions. The University should perform a comprehensive review of all terminated staff to ensure that the University's Security Officer has removed their access. Going forward, the University should follow the current policy in place and remove access within one business day of the effective termination date.

Strengthen Controls over Reporting Federal Expenditures

We found the University erroneously omitted \$1.2 million in expenditures from the data they submitted for the Schedule of Expenditures of Federal Awards included in the Commonwealth's Single Audit Report due to an error in the query they used to extract the data from Banner. In addition, the University's Financial Reporting and Grants and Contracts units did not detect this error through their review and reconciliation processes. We recommend the University develop and implement procedures to strengthen the controls surrounding the review and reconciliation of federal expenditure data.

Ensure Title IV Refund Calculations are Accurate

The Student Financial Aid Office used incorrect dates to calculate refunds of Title IV funds for fall 2009 and spring 2010 student withdrawals. When calculating the length of the semester, financial aid office staff used the last day of classes rather than the last day of exams as the official end of each semester. This error caused refund miscalculations for 11 of the 16 students selected for test work who officially withdrew during fall 2009 and spring 2010. For the return of Title IV funds calculation purposes, a week of instructional time is where at least one day of instruction or exams occurs or, after the last day of classes, at least one day of study for final exams occurs.

Subsequent to receiving our finding, the University reviewed all fall 2009 and spring 2010 calculations and returned \$6,006 to the federal programs. Management should also review Title IV procedures and implement a secondary review of the calculation and entry into their financial aid accounting system of critical data to ensure accuracy in the Title IV refund calculations and to prevent future errors.



Commonwealth of Virginia

Auditor of Public Accounts

Walter J. Kucharski
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

June 30, 2011

The Honorable Robert F. McDonnell
Governor of Virginia

The Honorable Charles J. Colgan
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
Virginia State University

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

We have audited the financial statements of the business-type activities and aggregate discretely presented component units of **Virginia State University** as of and for the year ended June 30, 2010, which collectively comprise the University's basic financial statements and have issued our report thereon dated June 30, 2011. Our report includes a reference to other auditors. We conducted our audit in accordance with 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. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of the University, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

Internal Control Over Financial Reporting

In planning and performing our audit, we considered the University's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University'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.

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 deficiencies, significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above. However, we identified certain deficiencies in internal control over financial reporting which are described in the section titled "Audit Findings and Recommendations," that we consider to be significant deficiencies in internal control over financial reporting. 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.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the 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. Instances of noncompliance and other matters, entitled "Improve Oracle Database Security," "Approve and Implement Information Security Program," "Strengthen Access Controls over eVA," and "Ensure Title IV Refund Calculations are Accurate" are described in the section titled "Audit Findings and Recommendations."

The University's response to the findings identified in our audit is included in the section titled "University Response." We did not audit the University's response and, accordingly, we express no opinion on it.

Status of Prior Findings

The University has made progress, but has not completed corrective action with respect to the previously reported findings "Improve Oracle Database Security" and "Approve and Implement Information Security Program". Accordingly, we included these findings in the section entitled titled "Audit Findings and Recommendations." The University has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Report Distribution and Exit Conference

The "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters" is intended solely for the information and use of the Governor and General Assembly of Virginia, the Board of Visitors, and management, and is not intended to be and should not be used by anyone, other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

We discussed this report with management at an exit conference held on July 22, 2011.

AUDITOR OF PUBLIC ACCOUNTS

SAH/clj



VIRGINIA STATE UNIVERSITY

P.O. Box 9213

PETERSBURG, VIRGINIA 23806

(804) 524-5995

(804) 524-5347 FAX

David J. Meadows

Vice President for Administration & Finance

TDD (804) 524-5487

July 25, 2011

Mr. Walter J. Kucharski
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218-1295

Dear Mr. Kucharski:

Virginia State University (VSU) has reviewed the Auditor of Public Accounts' (APA) report on Internal Control over Financial Reporting and on Compliance and Other Matters for the fiscal year ended June 30, 2010. The University appreciates the opportunity to respond to the findings and recommendations. In accordance with Government Auditing Standards, VSU provides the following response for inclusion in the report:

AUDIT FINDING AND RECOMMENDATIONS

Improve Oracle Database Security

VSU concurs that the Oracle database security in Oracle 10g needs to be improved and plans to upgrade from Oracle 10g to Oracle 11g by August 31, 2011. As we upgrade to the Oracle 11g database, Technology Services Management has taken the steps necessary to ensure that the Oracle database security is in full compliance with the University policies and procedures and the Commonwealth IT Security Standards. Specifically, the Chief Information Security Officer (CISO) has reviewed and approved Oracle 11g database baseline security configuration and password management using CIS Benchmark standards. Additionally, a Business Continuity Professional is working with the Technology Services Infrastructure team to develop recovery scripts for applications and systems.

Approve and Implement Information Security Program

VSU concurs that Technology Services Management and Chief Information Security Officer (CISO) have made progress in implementing its information security program in order to consistently protect sensitive data and comply with the Commonwealth's information security standards. The new Chief Information Officer (CIO) is reviewing the information security program and will draft plans to bring VSU into compliance with the Commonwealth IT Security Standard. A Business Continuity Professional will continue to work closely with the Technology Services team and CISO to complete the draft comprehensive IT Disaster Recovery Plan (DRP) and draft IT Continuity Operations Plan (COOP). These two documents will address the Business Impact Analysis (BIA), Risk Assessments, and IT System and Data Classification.

The next steps involve performing test drills and exercises to ensure that the IT data and system backups and restoration plans are properly tested and IT staff members are properly trained on disaster recovery roles and responsibilities as it relates to DRP and COOP.

Strengthen Access Controls over eVA

The University has performed a comprehensive review of terminated staff to ensure that access has been terminated in eVA. It has also instituted measures to ensure terminated staff are immediately identified and the appropriate forms are provided to the Department of General Services (DGS) within 24 hours of termination. Next steps involve seeking delegated authority to remove eVA access for terminated staff.

Strengthen Controls over Reporting Federal Expenditures

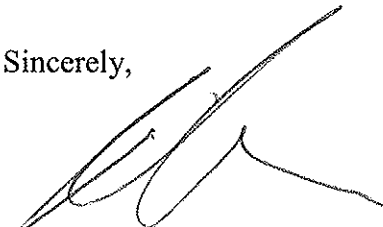
The University concurs that there was an error in the Schedule of Expenditures of Federal Awards (SEFA) for the fiscal year ended June 30, 2010. To prevent this error from repeating, an additional step has been added to the reconciliation process. Also, management will perform a more stringent review.

Ensure Title IV Refund Calculations are Accurate

As noted in the audit comment, the University instituted corrective actions immediately upon receiving this audit comment. In addition to reviewing the fall 2009 and spring 2010 calculations and making the necessary refunds to the federal program, new policies and procedures were implemented to prevent a recurrence of this finding.

Virginia State University is committed to addressing these audit findings and recommendations. We would like to thank you and your staff for your continued collaboration and support and look forward to our FY2011 audit.

Sincerely,



David J. Meadows
Vice President for Administration and Finance

cc: Dr. Keith T Miller, Jr., President
Mr. David A Von Moll, State Comptroller
The Honorable Gerard Robinson, Secretary of Education
Mr. Daniel Timberlake, Director of Planning and Budget

VIRGINIA STATE UNIVERSITY
Petersburg, Virginia

BOARD OF VISITORS
As of June 30, 2010

Earnest J. Edwards
Rector

Alfred J. Cade
Vice Rector

Katherine E. Busser
Secretary

Jerry Bias	Maureen D. Massey
Erika T. Davis	E. Ray Murphy
Felix Davis, Jr.	Daphne M. Reid
Mary H. Futrell	James H. Starkey
Christopher H. Holden	Barbara Steverson
Richard D. Legon	Spencer L. Timm

Dr. Ben U. Nwoke, Faculty Member Representative
Ms. Cassandra Campbell, Student Representative

ADMINISTRATIVE OFFICIALS
As of June 6, 2011

Keith T. Miller
President

Robert L. Turner, Jr.
Vice President for Development

W. Weldon Hill
Vice President for Academic Affairs

Michael Shackelford
Vice President of Student Affairs

David J. Meadows
Vice President for Administration and Finance