VIRGINIA STATE UNIVERSITY

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2009

APA
Auditor of
Public Accounts
COMMONWEALTH OF VIRGINIA

AUDIT SUMMARY

Our audit of the Virginia State University for the year ended June 30, 2009, found:

- the financial statements are presented fairly, in all material respects, with generally accepted accounting principles;
- internal control matters that are necessary to bring to management's attention;
- instances of noncompliance required to be reported under Government Auditing Standards;
- the University has not taken adequate corrective action with respect to the previously reported finding titled "Strengthen Controls over Capital Asset Reporting;" therefore, that finding is repeated in this year's report; and
- the University did take adequate 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, 2009, and issued our report thereon, dated June 23, 2010. Our report, included in the Virginia State University's Annual Financial Report 2008 - 2009, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the Virginia State University's website at www.vsu.edu.

–TABLE OF CONTENTS–

Pages

AUDIT SUMMARY

AUDIT FINDINGS AND RECOMMENDATIONS 1-3

INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS 4-6

UNIVERSITY RESPONSE 7-9

UNIVERSITY OFFICIALS 10

AUDIT FINDINGS AND RECOMMENDATIONS

INTERNAL CONTROL AND COMPLIANCE MATTERS

Improve Database Management

The University does not protect its databases storing sensitive data according to industry best practices and Commonwealth Security Standards. Specifically, the University needs to improve password management, user profile setup, and system auditing. We have communicated the details of these weaknesses to management in a separate document to management marked Freedom of Information exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of the security system.

By not documenting, training, and implementing its security requirements for its databases, the University cannot assert that it has properly protected its sensitive data and consistently managed its databases. Therefore, we recommend that the University develop and implement policies, procedures, and standard configuration guidelines for its databases, and ensure that its technical staff is trained and aware of these requirements.

Improve Firewall Management

The University does not properly manage the firewall that protects its internal administrative network and servers from unauthorized access according to industry best practices and Commonwealth Security Standards. We have communicated the details of these weaknesses to management in a separate document to management marked Freedom of Information exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of the security system. We recommend that the University document the security settings for the firewall, develop a change management approval process, and management should periodically review the rules and settings to ensure that its firewall is properly configured and provides a robust barrier against attack.

Approve and Implement Updated Information Security Program

Virginia State University needs to implement its updated information security program in order to provide consistent protection of its sensitive data and comply with the Commonwealth's information security standard. Since our last review, the University hired a full-time Information Security Officer (ISO), who drafted new information security policies and procedures. Until management approves and communicates these policies and procedures to the University community through training, the ISO cannot enforce the data safeguard requirements outlined in the information security program. The University should finalize, approve, and implement its information technology security policies and procedures. It should also include this information in its security awareness training program to ensure that staff are aware of their security responsibilities.

Strengthen Controls over Capital Asset Reporting

The University must continue to improve their processes over capital asset reporting. Since the prior audit, the University has made some improvements in this area. However, during the audit, we found reporting errors including duplicate capitalization of library books and misclassification of capital assets categories although not to the extent of the errors we noted in the prior audit. In addition, we continue to note areas for improvement in the reconciliation process for construction in progress.

We recognize that the University is still in the process of making improvements in their controls surrounding capital asset reporting including reassigning responsibilities within its accounting divisions. We recommend the University continue its efforts in this area. Specifically, the University should continue to review the capital asset reporting process and ensure it has developed, documented, and implemented sufficient policies and procedures to prevent misstatements in the financial statements.

The policies and procedures should address reconciliations, timely identification of non-capital expenses, and evaluation of project expenses occurring subsequent to capitalization. We also recommend that the Financial Reporting Division continue to work with other divisions involved in the process to ensure they have adequate controls over their processes related to capital assets.

Strengthen Access Controls over Banner

Virginia State University should improve several areas related to Banner access and controls.

Remove Access Timely

The Office of Information Technology (OIT) did not timely delete Banner access for terminated employees. According to University policy, the OIT staff should remove access for terminated employees within one day of the date of termination. However, we noted delays in removing access that ranged from 25 days to over 18 months. Terminated employees could potentially access Banner to enter and process false or fraudulent transactions. The OIT staff should perform a comprehensive review of all terminated employees to ensure they have removed their access from any critical University systems. Going forward, the OIT should follow the current policy in place and remove access within one business day of the effective termination date. The University's Internal Audit Division noted this issue prior to our review. Therefore, the University has already begun taking corrective actions in this area.

Ensure Access is Appropriate Based on Job Responsibilities

The OIT assigned users access to Banner that was not appropriate based on their job responsibilities. Banner allows the University to create *CLASSES*, which represents a group of employees that can perform certain functions within the application. These *CLASSES* allow the University to grant access to employees without having to create a customized access profile each time an employee comes to work, receives a promotion or some other personnel action occurs.

Banner also comes with a number of commonly used CLASSES, which the University can change. However, some of these predefined CLASSES are Supervisors, which allows them to add, delete, change, and approve transactions without any oversight. Therefore, when implementing Banner making sure that the University either creates or uses the appropriate CLASSES is essential for establishing internal control and also requires and at least an annual review of employees CLASSES to ensure the maintenance of good internal control.

During our review we found the OIT assigned users to classes that were not appropriate for their job responsibilities. We also found individuals having access to the correct Banner class; however, the class included access to forms that was inappropriate for that particular Banner class. In addition, the OIT assigned users to nine classes that are not in use by the University. Finally, we found a user ID that OIT assigned to VSU created classes, which the original Banner software uses for implementation purposes only. This user ID provides unrestricted access to numerous Banner modules and is part of the testing process of applications and modules before and during Banner implementation.

Giving employees access to classes or forms that are not associated with their job responsibilities could lead to employees entering erroneous information into Banner, improperly approved transactions, and improper segregation of duties. Although the University had assigned some individuals access to inappropriate classes, the University relied on the extra security layers built into Banner that did not allow those employees to change information within those classes. However, cleaning up the user classes to remove inappropriate access will make it easier for the University to perform annual user access reviews.

In December 2009, the Database Administrator implemented a "clean up" process of Banner. This process involves reviewing classes to ensure the correct forms are included and also removing unnecessary classes. We recommend the University continue with this effort and do so periodically until it is comfortable with the forms within those classes. We also recommend the University perform periodic reviews of user access to ensure access is appropriate.

Going forward, the University should only assign an employee access if it is clear that the requested class is necessary to perform job responsibilities. Supervisors should only request access needed for specific duties and explain why the employees need access to the classes requested. The Manager of Financial Requirements and Procedures should ensure the classes coordinate to the responsibilities of each user. The University should closely monitor and restrict access to the user IDs included in the original Banner software for testing and limit this access to only essential information technology personnel.

EFFICIENCY ISSUE

Utilize Banner Efficiencies

Banner offers more sophisticated functionality including recurring accounts payable and journal voucher processing and workflow that the University is currently not using. These functions could improve the efficiency of the University's operations and reduce paperwork. Using the recurring accounts payable feature would allow the University to have recurring payments, such as rent or lease payments, automatically post each month. With recurring journal vouchers, the University would be able to improve efficiency by programming the system to post automatically on pre-defined dates those journal vouchers that occur on a regular basis. The Banner workflow feature would allow the University to initiate a transaction and process it through the necessary approval channels within Banner, without having to maintain paper documentation.

At this time the University has decided not to use the recurring accounts payable and journal vouchers forms since it believes it will impact its Banner automatic interfaces with the Commonwealth Accounting and Reporting System. In addition, while the University agrees it could gain efficiencies by utilizing some of the Banner workflow products, it has decided to postpone implementation of those products until after it has implemented an upgrade to Banner and has funding to implement the workflow products. We recommend that the University continue to evaluate opportunities to improve their efficiency and reduce paperwork by utilizing Banner's workflow and recurring entries functions once they implement the Banner version upgrade.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

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

June 23, 2010

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, 2009, which collectively comprise Virginia State University's basic financial statements and have issued our report thereon dated June 23, 2010. Our report was modified to include 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.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control over financial reporting. We consider the deficiencies described in the section titled "Internal Control and Compliance Matters", to be significant deficiencies in internal control over financial reporting.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in the internal control over financial reporting that might be significant deficiencies and, accordingly, would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, we believe that none of the significant deficiencies described above is a material weakness.

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 Database Management", "Improve Firewall Management", and "Approve and Implement Updated Information Security Program" are described in the section titled "Internal Control and Compliance Matters".

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 not taken adequate corrective action with respect to the previously reported finding "Strengthen Controls over Capital Asset Reporting". Accordingly, we include this finding in the section entitled "Internal Control and Compliance Matters." The University has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Exit Conference and Report Distribution

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 June 24, 2010.

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

June 29, 2010

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) Internal Control and Compliance Matters and the Efficiency Issue for the fiscal year ended June 30, 2009. The University appreciates the opportunity to respond to the findings and recommendations. In accordance with Government Auditing Standards, VSU is providing this response for inclusion in your published report.

INTERNAL CONTROL AND COMPLIANCE MATTERS

Improve Database Management

VSU will continue its efforts to extend the Banner system boundary to include the Financial Reporting process and its associated IT resources. All associated security artifacts will be updated to ensure proper security controls are in place, as well as timely recovery after a disaster. VSU will also follow its logical access control procedures for this process to ensure that this process does not provide unauthorized personnel access to data that has not been approved for them.

Improve Firewall Management

VSU concurs with this finding. The University will document the security settings for the firewall, develop a change management approval process, and periodically review the rules and settings to ensure a secure computing environment.

"VSU: Education, Research and Community Service in Central and Southside Virginia..."

Approve and Implement Updated Information Security Program

The University's latest Information Security Policy was revised on January 19, 2010 and approved by the President of the University on February 3, 2010. This policy delineates the roles and responsibilities for management and protection of the University's IT systems and data, as required by the Information Technology Information Security Policy (SEC-501). This revised policy along with twelve (12) IT Security policies is available on the University's website and these policies will be included in the IT Security Awareness Training program to ensure staff members are aware of their responsibilities.

Strengthen Controls over Capital Asset Reporting

Although the University made changes and improvements in this area during FY2009, it had not completed all of the necessary improvements by the end of the fiscal year. To ensure all aspects of the capital asset reporting function is addressed, the University assembled a work team that is responsible for reviewing, developing, documenting, and implementing processes, policies and procedures, and related controls that will correct and improve the entire process. In addition, meetings will be held periodically with all departments involved in the capital asset reporting function to ensure the data is complete and current.

Strengthen Access Controls over Banner

Remove Access Timely

The University understands the importance of removing access in a timely manner. The Office of Information Technology, in conjunction with the Database Administrator and Banner Security Managers, will perform a periodic comprehensive review of all terminated employees to ensure their access to any critical University system is removed in a timely manner. The University will coordinate and communicate with business departments to ensure that access is removed within one business day of the effective termination date.

Ensure Access is Appropriate Based on Job Responsibilities

The Banner Security Managers and Database Administrator will perform periodic comprehensive review of users' access to the Banner system and data to ensure that users only have the access necessary to perform their functional responsibilities.

EFFICIENCY ISSUE

The University appreciates the Auditor's input and recommendation related to the efficiency issue. After a successful upgrade to Banner and as funding and resources are available, the University will explore the feasibility of implementing Banner's workflow products. Further, the University will remain focused on enhancing operations and improving efficiencies.

Virginia State University remains committed to addressing the findings and recommendations. We would like to thank you and your staff for your continued collaboration and support in improving the University. We look forward to next year's audit.

Sincerely,

David J. Meadows
Vice President for Administration and Finance

cc: Dr. Eddie N. Moore, 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

ADMINISTRATIVE OFFICIALS
As of June 23, 2010

Eddie N. Moore, Jr.
President

Robert L. Turner, Jr.
Vice President for Development

W. Weldon Hill
Interim Vice President for Academic Affairs

Michael Shackelford
Vice President of Student Affairs

David J. Meadows
Vice President for Administration and Finance