

VIRGINIA MILITARY INSTITUTE

**REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2008**

APA

**Auditor of
Public Accounts**

COMMONWEALTH OF VIRGINIA

AUDIT SUMMARY

Our audit of the Virginia Military Institute for the year ended June 30, 2008, found:

- the financial statements are presented fairly, in all material respects;
- an internal control matter necessary to bring to management's attention; and
- no instances of noncompliance or other matters required to be reported under Government Auditing Standards.

We have audited the basic financial statements of the Virginia Military Institute as of and for the year ended June 30, 2008 and issued our report thereon, dated April 13, 2009. Our report, included with the Institute's basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the Institute's website at www.vmi.edu.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL FINDING AND RECOMMENDATION	1
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	2-3
INSTITUTE RESPONSE	4
INSTITUTE OFFICIALS	5

INTERNAL CONTROL FINDING AND RECOMMENDATION

Improve Information Systems Security Program Documentation

The Virginia Military Institute (Institute) needs to enhance its Information Systems Security Program documentation. The Institute should fix a time period in its policies for the removal of employee's user accounts to sensitive systems when an employee leaves, and document its policies and procedures for security over credit card transactions.

Removing user accounts with access to sensitive data promptly after employees terminate will improve how the Institute safeguards its data. The Institute's lack of a clear policy resulted in inconsistent and subjective interpretation of when to remove user accounts with access to sensitive information after an employee's termination. We recommend that the Institute clarify its policy by indicating a specific time period by which the Department of Information Technology will close user accounts upon employee termination.

Since the Institute accepts and processes credit cards, it has to follow the Payment Card Industry Data Security Standards. Non-compliance with these standards may result in fines or suspension of the Institute's privilege to process credit cards. During our review, we found that the Institute is in the process of implementing these standards and we encourage that the Institute continue to dedicate the necessary resources to complete implementation and provide appropriate training to affected employees as soon as possible.



Commonwealth of Virginia

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

Walter J. Kucharski, Auditor

April 13, 2009

The Honorable Timothy M. Kaine
Governor of Virginia

Board of Visitors
Virginia Military Institute

The Honorable M. Kirkland Cox
Chairman, Joint Legislative Audit
and Review Commission

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 the **Virginia Military Institute** as of and for the year ended June 30, 2008, which collectively comprise the Institute's basic financial statements and have issued our report thereon dated April 13, 2009. 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 Institute, 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 Institute'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 Institute's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Institute's internal control over financial reporting.

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 deficiency entitled "Improve Information Systems Security Program" which is described in the section titled "Internal Control and Compliance Findings and Recommendations", to be a significant deficiency.

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 the significant deficiency described above is not a material weakness.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Institute'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.

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

Status of Prior Findings

The Institute has taken adequate corrective action with respect to audit findings reported in the prior year.

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 April 24, 2009.

AUDITOR OF PUBLIC ACCOUNTS

JLN/alh

VIRGINIA MILITARY INSTITUTE

LEXINGTON, VIRGINIA 24450-0304

OFFICE OF THE SUPERINTENDENT

Office 540-464-7311

Fax 540-464-7660

Voice/TDD 540-464-7616

30 April 2009

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

Dear Mr. Kucharski:

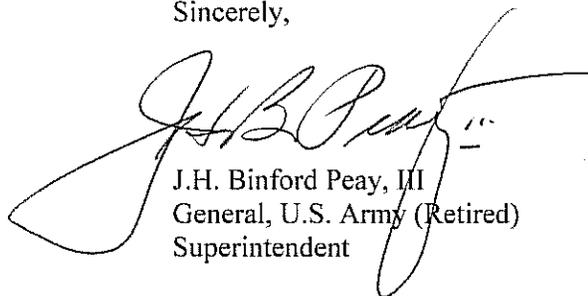
During the course of our 2008 fiscal year audit, your staff issued an internal control and compliance finding noting the Institute's need to enhance certain Information Systems Security Program documentation. Specifically, the APA directed the Institute to fix a time period in its policies for the removal of employee's user accounts to sensitive systems when an employee leaves, and document its policies and procedures for security over credit card transactions.

The current VMI Clearance Policy requires a supervisor to report to the Human Resources Office the planned separation of an individual or the actual separation of an individual immediately upon knowledge of the planned or actual separation. The Human Resources Office enters a transaction to terminate systems access on the separation date. Although the APA did not note any discrepancies during the audit, VMI understands the APA's concern to specify time frames for notification. Accordingly, VMI will revise the policy to require a supervisor to notify the Human Resources Office within 72 hours of learning of a planned separation from employment. The Human Resources Office will key the transaction within 72 hours of receiving the notification. In the event of an employee's unforeseen termination from employment, the supervisor must notify the Human Resources Office of the termination no later than the close of business on the following business day. The Human Resources Office must key the transaction no later than the close of business on the next business day following notification.

As noted in your finding, the Institute is in the process of implementing Payment Card Industry Data Security Standards. The Security Standards Council issued these standards or requirements for entities that accept credit or debit cards as a method of payment. The Institute has addressed most of these standards and much documentation is already embedded within other Institute information security policies. We will complete our policies and procedures to address these standards and consolidate them with those already implemented.

Thank you for the opportunity to provide our response to this finding.

Sincerely,



J.H. Binford Peay, III
General, U.S. Army (Retired)
Superintendent



VIRGINIA MILITARY INSTITUTE

BOARD OF VISITORS

Thomas G. Slater
President

Paul D. Fraim
Vice President

James E. Rogers
Vice President

Elizabeth D. Camp	Anthony Q. McIntosh
Lie-Ping Chang	Bruce C. Morris
P. Wesley Foster, Jr.	G. Marshall Mundy
Ronald H. Griffith	Robert B. Newman
Patricia P. Hickerson	William A. Paulette
Michael W. Maxwell	George P. Ramsey III
Robert L. McDowell	W. Gregory Robertson

Benjamin F. Kimsey, Cadet Representative

Michael M. Strickler
Secretary of the Board of Visitors

OFFICERS

J.H. Binford Peay III
Superintendent

Robert L. Green
Deputy Superintendent for Finance, Administration and Support

Robert W. Gilbert
Comptroller