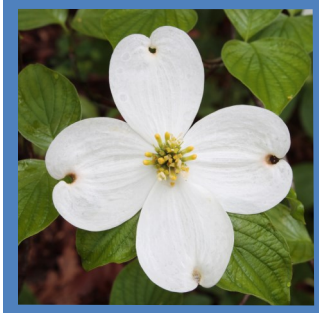


VIRGINIA MILITARY INSTITUTE

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2023

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Military Institute (Institute) as of and for the year ended June 30, 2023, and issued our report thereon, dated August 1, 2024. Our report, included in 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. Our audit found:

- the financial statements are presented fairly, in all material respects;
- deficiencies in internal control and its operation necessary to bring to management's attention including one related to reporting of subscription based information technology arrangements that we consider to be a material weakness in internal control;
- instances of noncompliance or other matters required to be reported under Government Auditing Standards; and
- adequate corrective action with respect to prior audit findings and recommendations identified as complete in the Findings Summary included in the Appendix.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audits as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendation.

-TABLE OF CONTENTS-

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Controls over Reporting of Subscription Based Information Technology Arrangements
Type: Internal Control
Severity: Material Weakness

Virginia Military Institute's (Institute's) Office of Finance and Budget (Finance and Budget) did not fully comply with the requirements of Governmental Accounting Standards Board (GASB) Statement No. 96, which prescribes the applicable accounting standards for proper accounting and financial reporting of subscription-based technology arrangements (SBITAs). This standard was new and complex, requiring significant preparation and effort from Finance and Budget prior to implementation. However, even with this effort, Finance and Budget did not complete or document an accurate analysis of contracts or expenses that could represent SBITAs. During the audit, we identified the following internal control deficiencies:

- Finance and Budget improperly applied the threshold to determine if an expense was a potential SBITA and, as a result, excluded expenses that it should have evaluated. In our sample of nine expenses, we identified two (22%) that Finance and Budget should have evaluated as a potential SBITA.

- Finance and Budget's mechanism to track potential SBITAs did not include adequate documentation to support why they excluded potential SBITAs from their analysis. In our sample of nine expenses, we identified one (11%) for which Finance and Budget did not have adequate documentation of their evaluation.

- Finance and Budget's mechanism to calculate the SBITA asset, liability, and amortization did not include adequate documentation to show that they considered the required elements to correctly perform the calculation.

- Finance and Budget did not document a justification for the interest rate used to calculate the SBITA asset and liability.

- In our sample of three SBITAs, we found one (33%) SBITA that Finance and Budget improperly identified as a long-term SBITA and recorded within the financial statements. This resulted in a misstatement of $265,418.

- In our sample of five SBITAs, we found two (40%) SBITAs that Finance and Budget should have evaluated as a long-term SBITA to determine if it exceeded the threshold for recording.

In addition to the deficiencies noted above, Finance and Budget incorrectly recorded the SBITA liability by recording amortization instead of the principal in the financial statements. This resulted in a misstatement of $135,763 in current subscription liability and $327,357 in non-current subscription liability. Finance and Budget also did not include all the information required by the standard in the SBITA related footnote.

The Commonwealth Accounting Policies and Procedures (CAPP) Manual Topics 31305 and 31310 state that each agency should implement internal control procedures to ensure that all potential contracts to use nonfinancial assets are properly evaluated to determine if the transactions are SBITAs and to ensure that agencies properly classify all SBITAs as short-term or long-term. Finance and Budget's policies and procedures were not adequate to ensure proper and complete identification and evaluation of all potential SBITAs. Additionally, Finance and Budget did not have sufficient resources to adequately consider all requirements set forth by GASB Statement No. 96.

Misapplication or misinterpretation of GASB Statement No. 96 can result in inaccurate financial reporting, which can affect long-term planning and the decision making of individuals or other institutions that rely on the reported financial information. While the internal control deficiencies above did not result in any required adjustments to the financial statements, the deficiencies create an environment in which there is a reasonable possibility that Finance and Budget will not prevent or detect a significant error or omission that affects the reliability of the financial statements on a timely basis. As a result, we consider this to be a material weakness in internal controls.

Finance and Budget should develop and implement more robust policies and procedures to ensure the proper identifying, tracking, recording, and reporting of SBITAs. Additionally, Finance and Budget should dedicate the necessary resources to gain an adequate understanding of GASB Statement No. 96 requirements and conduct and document a thorough review of its current contracts to properly identify potential SBITAs. Implementing effective corrective action will help ensure accurate and complete financial reporting in accordance with GASB Statement No. 96 when preparing financial statements for future periods.

Ensure Proper Documentation of Bank Reconciliations

Type: Internal Control
Severity: Significant Deficiency
First Reported: Fiscal Year 2021

The Institute did not adequately document the preparation and review of the monthly bank reconciliation process. For all three reconciliations tested during the audit, the Institute could not provide evidence to support timely preparation or to support proper review by someone other than the preparer.

The Institute's Accounting Policies and Procedures, Section 20100, states that the Finance and Budget should reconcile accounting information, bank accounts, and transactions between modules monthly. The Institute did not adequately document the preparation and review of the monthly bank reconciliations due to staffing shortages. Without sufficient documentation to ensure the preparation and review of the bank reconciliations, there is an increased risk that Finance and Budget will not detect or be able to correct errors timely. This could lead to a potential misstatement of the cash balance in the Institute's financial statements.

The Institute should adequately document and timely complete reconciliations in accordance with the Institute's policies and procedures and best practices. The Institute implemented a corrective action plan as of June 30, 2023, which we will review during the fiscal year 2024 audit.

Improve Information Technology Risk Management and Contingency Planning Program

Type: Internal Control and Compliance
Severity: Significant Deficiency

The Institute does not conduct aspects of its information technology (IT) risk management and contingency planning program in accordance with the Commonwealth's Information Security Standard, SEC501 (Security Standard). IT risk management documents include the Institute's Business Impact Analysis (BIA), IT system and data sensitivity classifications (sensitivity classifications), and IT system risk assessments (RA). Contingency planning documents include the Institute's Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP). Specifically, the following weaknesses exist:

- The Institute does not use information documented in the BIA as the primary input to its other IT risk management and contingency planning documents. The BIA delineates the steps necessary for organizations to identify their business functions, identify those that are essential to the organization's mission, and identify the resources that are required to support the essential functions. The Security Standard requires the Institute to use the IT information documented in the BIA report as a primary input to sensitivity classifications, RAs, COOP, and System Security Plans (SSPs) (*Security Standard, section 3 Business Impact Analysis*). As a result, the Institute does not consistently define essential information between its BIA and COOP, including:

    - Mission essential functions (MEF)
    - Primary business functions (PBF)
    - IT systems and resources that support each MEF and PBF
    - Recovery time objectives (RTO)
    - Recovery point objectives (RPO)

    The inconsistent information across its IT risk management and contingency planning documentation may delay the Institute recovering its mission essential functions and supporting IT systems in the event of a disruption or disaster. The Institute conducted a BIA based on the information in its Institute-wide COOP instead of conducting the BIA first when developing its IT risk management and contingency planning documents. This was due to a misunderstanding in the Security Standard's requirements and development process.

- The Institute did not conduct an effective test of its COOP and DRP. Additionally, the Institute did not document the results of its test on an annual basis. While the Institute performed a test during the fiscal year, the scenario and objectives of the test were not adequate to test the COOP procedures and recovery of systems and business operations within RTO and RPO requirements as the Institute excluded contingency planning scenarios. The Institute-wide COOP, as well as the Security Standard, require the Institute to conduct annual exercises to

test the IT Disaster Recovery components and elements of the COOP to validate and assess their effectiveness and the overall readiness of the Institute to execute its contingency plans. Additionally, the Institute is required to conduct a periodic review, reassessment, testing, and revision of the IT DRP to reflect changes to the Institute's environment (*Security Standard, sections CP-1-COV-1 Contingency Planning Policy and Procedures, CP-4 Contingency Plan Testing and Exercises)*. Without adequate COOP and DRP testing, the Institute increases the risk that staff are not prepared to respond to various scenarios that may occur and interrupt normal operations and system availability.

- The Institute did not include contingency procedures for one of its three MEFs within the Institute-wide COOP. The Security Standard requires the Institute to identify essential mission and business functions and associated contingency requirements. Additionally, the Security Standard requires the Institute address maintaining essential missions and business functions despite an information system disruption, compromise, or failure (*Security Standard, section CP-2 Contingency Plan*). By not defining contingency procedures or identifying the resources required to enable the contingency procedures, the Institute's staff may be unprepared and ill-equipped to maintain MEFs and PBFs in the event of a disaster. The lack of procedures resulted from an oversight when documenting contingency procedures within the Institute's COOP.

- The Institute did not conduct annual reviews of its IT risk management and contingency planning documentation in accordance with the Security Standard to validate the information is accurate and revised as needed to reflect the Institute's current IT environment (*Security Standard, sections 3.2 Business Impact Analysis, CP-1 Contingency Planning Policy and Procedures, CP-2 Contingency Plan, PL-2 System Security Plan, RA-1 Risk Assessment Policy and Procedures)*. Specifically, the Institute did not conduct annual reviews of the following:

  - BIA (no documented review history)
  - SSPs (last reviewed in August 2021)
  - RAs and risk treatment plans (last reviewed in September 2022)
  - IT COOP and DRP (last reviewed in December 2021)
  - Institute-wide COOP (last reviewed in September 2022)

  By not reviewing and updating its IT risk management and contingency planning documentation, the Institute increases the risk that the documents do not reflect its current environment and may delay recovery processes in the event of a disaster or disruption. The Institute did not review the documents due to limited staffing resources.

- The Institute does not include certain IT risk management requirements within its IT-100 Policy as required by the Security Standard. Specifically, the Institute does not include requirements to conduct a BIA and use it as the primary input to its Sensitivity Classifications, RA, COOP and SSP. Additionally, the Institute does not define requirements to conduct security classification based on confidentiality, integrity, and availability (*Security Standard, sections: 3 Business Impact* Analysis*; 4.1-2 IT System and Data Sensitivity Classification*). By

not ensuring the IT-100 Policy aligns with the Security Standard, the Institute is unable to consistently conduct and enforce processes to maintain current risk management and contingency documents. The Institute's misunderstanding of Security Standard requirements for policies and procedures led to the IT-100 Policy lacking certain requirements.

The Institute should re-evaluate its BIA and use it as a primary input for its other IT risk management and contingency planning documents. The Institute should also ensure it identifies and documents contingency procedures for its MEFs and PBFs and conduct an effective test of the COOP and DRP that tests the effectiveness of the procedures to recover the business functions and supporting systems within the RTO and RPO requirements. Additionally, the Institute should review and revise its IT-100 Policy to include the necessary requirements outlined in the Security Standard and review its IT risk management and contingency planning documentation at least annually to ensure it reflects the Institute's current environment. This will help ensure the confidentiality, integrity, and availability of sensitive and mission essential systems and business functions.

Improve Physical and Environmental Security Program Documentation

Type: Internal Control and Compliance
Severity: Significant Deficiency

The Institute does not include certain elements within its IT-100 Policy. In addition, the Institute has not implemented some minimum physical and environmental security requirements in its IT-100 Policy and the Security Standard, to protect its sensitive IT systems. The Institute has one server room that houses IT infrastructure assets that contain confidential and mission critical data. The following physical and environmental security control weaknesses exist:

- The Institute did not document its review of the facility access list to verify its staff continued need to access its server room. The IT-100 Policy, which is based on the Security Standard, requires the Institute to review the list of personnel with access to all IT resources whenever an individual's role changes or the user leaves the Institute, but at least annually (IT-100 *Policy, section C. Procedures – IT Department and Server Room Physical Access Controls; Security Standard, section: PE-2 Physical Access Authorizations*). Without documenting its review, the Institute does not have a record that a review was conducted and increases the risk for a user to have unauthorized access to secure areas.

- The Institute did not document its reviews of physical access logs or visitor access logs to its server room. Additionally, the Institute does not retain visitor access logs for at least one year. The IT-100 Policy requires the Institute to review the physical access logs at least once every sixty days and review the visitor access logs monthly (IT-100 *Policy, section C. Procedures Physical Security*; *Security Standard, sections: PE-6 Monitoring Physical Access, PE-8 Access Records*). The Security Standard also requires the Institute to maintain visitor access records to the facility where the information system resides for a minimum period of one year (*Security Standard, section: PE-8 Access Records)*. Without a documented record of review of physical access or visitor access to secure facilities and by not retaining visitor access records for a minimum of one year, the Institute increases the risk that it will not

detect unauthorized users that may access secure locations and increases the risk of not identifying abnormal log entries and patterns that may signify a breach.

- The Institute does not include certain requirements and procedures within its IT-100 Policy as required by the Security Standard. Specifically, the Institute does not require retaining visitor access logs for at least one year and does not outline requirements and procedures for using surveillance and intrusion detection systems to monitor access to the server room. The Security Standard requires the Institute to develop, document, and disseminate a physical and environmental protection policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination, and compliance, and procedures to facilitate the implementation of the physical and environmental protection policy (*Security Standard, sections: PE-1 Physical and Environmental Protection Policies and Procedures, PE-6 Monitoring Physical Access)*. Without adequate policies and procedures to govern physical and environmental security controls, the Institute increases the risk for personnel to inconsistently enforce and implement the necessary controls.

The Institute's lack of certain requirements and procedures within its IT-100 Policy led to the weaknesses above. Additionally, the Institute experienced turnover in its IT leadership positions, which led to its new leadership misunderstanding that the required controls and processes had not been implemented.

The Institute should review and update the IT-100 Policy to include the requirements of the Security Standard and develop procedures to support implementing an effective physical and environmental security program. The Institute should also document its reviews of facility access lists and access logs to ensure personnel consistently monitor restricted areas and identify suspicious events for future reference. Additionally, the Institute should retain its visitor access logs for a minimum of one year to detect patterns of unauthorized access or suspicious events. This will help ensure the confidentiality, integrity, and availability of its sensitive and mission critical data.

Improve Controls over Terminated Employees
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2020

During fiscal year 2023, Institute Human Resources personnel did not consistently and timely remove system access for terminated employees. In our review of 13 terminated employees, we determined Human Resources did not remove access within 24 hours upon termination for five employees (38%).

Section PS-4 of the Security Standard requires agencies to disable information systems access within 24 hours of employment termination. The Institute's General Order 35 – Personnel Clearance Procedures Policy (Policies and Procedures), states that "As soon as the immediate supervisor learns of the departure or planned departure of an employee or other individual covered by this policy, the supervisor must send (either electronically or by fax) the "Exit Alert" form to the Human Resources

Office." It is then the responsibility of Human Resources to enter the individual's separation date and account lock date within 72 hours of receiving the notification, whereby the Institute's accounting and financial reporting system will disable the individual's account as needed.

The underlying cause of these exceptions is the lack of communication between the supervisor of the terminated employee and Human Resources, as there is often a timing delay in which the supervisor alerts Human Resources of an employee's termination date. Additionally, the Institute's policies and procedures are not in accordance with the Security Standard, which mandates a 24-hour time frame to remove terminated employee system access.

Not removing terminated employees' system access in accordance with the Security Standard increases the Institutes' level of risk of unauthorized access to Institute computer systems and facilities. Human Resources should ensure the Institute's policies and procedures align with the Security Standard and enforce the policies and procedures within the Institute's departments. The Institute implemented a corrective action plan as of June 30, 2023, which we will review during the fiscal year 2024 audit.

Conduct Information Technology Security Audits

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

The Institute has not performed an IT security audit over its sensitive systems within three years. The Institute continues to search for an external audit firm to perform IT security audits of its sensitive systems in accordance with the Commonwealth's IT Security Audit Standard, SEC502 (IT Security Audit Standard).

The Institute's IT-100 Policy, which aligns with the IT Security Audit Standard, requires its on-premise sensitive systems to receive an IT security audit every three years. Additionally, the IT Security Audit Standard requires all IT security audits to follow an established audit framework, such as the Generally Accepted Government Auditing Standards (GAGAS) Yellow Book or American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards, assess the effectiveness of system controls, and measure compliance with the applicable Commonwealth IT Resource Management Policies and Standards (IT-100 Policy, IV. Risk Management section C, Procedures; IT Security Audit Standard, sections: 1.4 Scope and Frequency of IT Security Audits; 1.5 IT Audit Frameworks; 2.2 IT Security Scope).

During fiscal year 2022, the Institute reviewed the Virginia Association of State College & University Purchasing Professionals (VASCUPP) website and pre-selected a vendor but found the vendor contract did not meet all requirements in the IT Security Audit Standard. The delay in identifying an acceptable audit firm caused the Institute's limited progress with its corrective actions. Without conducting IT security audits over all sensitive systems at least once every three years, the Institute may not detect and mitigate weaknesses affecting its IT environment. Additionally, malicious parties can exploit the unmitigated weaknesses to compromise the Institute's sensitive systems.

The Institute should continue its efforts to find an external audit firm to conduct IT security audits of its sensitive systems in accordance with an acceptable audit framework. Additionally, the Institute should continue to ensure it specifies compliance requirements for outsourced work and maintain oversight of its external contractors to verify the work is completed as required. The Institute should also perform future IT security audits over its sensitive systems once every three years in accordance with the IT Security Audit Standard. This will help to ensure the confidentiality, integrity, and availability of the Institute's sensitive and mission critical data.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

August 1, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
Virginia Military Institute

Major General Cedric T. Wins
Virginia Military Institute

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 **Virginia Military Institute** (Institute) as of and for the year ended June 30, 2023, and the related notes to the financial statements, which collectively comprise the Institute's basic financial statements and have issued our report thereon dated August 1, 2024. Our report includes a reference to other auditors who audited the financial statements of the component units of the Institute, as described in our report on the Institute's financial statements. The other auditors, excluding those of VMI Research Laboratories, did not audit the financial statements of the component units of the Institute in accordance with Government Auditing Standards, and accordingly, this report does not include reporting on internal control over financial reporting or compliance and other matters associated with those component units of the Institute. Additionally, this report does not include the results of the other auditors' testing of internal control over financial reporting or compliance and other matters for VMI Research Laboratories, that are reported on separately by those auditors.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the Institute's internal control over financial reporting (internal control) as a basis for designing 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 Institute's internal control. Accordingly, we do not express an opinion on the effectiveness of the Institute's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control 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 section titled "Internal Control and Compliance Findings and Recommendations," we identified certain deficiencies in internal control that we consider to be a material weakness 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 titled "Improve Controls over Reporting of Subscription Based Technology Arrangements," which is described in the section titled "Internal Control and Compliance Findings and Recommendations," to 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 titled "Ensure Proper Documentation of Bank Reconciliations," "Improve Information Technology Risk Management and Contingency Planning Program," "Improve Physical and Environmental Security Program Documentation," "Improve Controls over Terminated Employees," and "Conduct Information Technology Security Audits," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," to be significant deficiencies.

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 financial statements. 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 section titled "Internal Control and Compliance Findings and Recommendations" in the findings and recommendations titled "Improve

Information Technology Risk Management and Contingency Planning Program," "Improve Physical and Environmental Security Program Documentation," "Improve Controls over Terminated Employees," and "Conduct Information Technology Security Audits."

The Institute's Response to Findings

We discussed this report with management at an exit conference held on August 19, 2024. Government Auditing Standards require the auditor to perform limited procedures on the Institute's response to the findings identified in our audit, which is included in the accompanying section titled "Institute Response." The Institute's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

The Institute has not taken adequate corrective action with respect to the prior reported findings and recommendations identified as ongoing in the Findings Summary included in the Appendix. The Institute has taken adequate corrective action with respect to prior audit findings and recommendations identified as complete in the Findings Summary included in the Appendix.

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 Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

AVC/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Ensure Compliance with Conflict of Interests Act	Complete	2021
Develop a Baseline Configuration for the Operating System Server Environment	Complete	2022
Improve Controls over Reporting of Subscription Based Technology Arrangements	Ongoing	2023
Ensure Proper Documentation of Bank Reconciliations	Ongoing	2021
Improve Information Technology Risk Management and Contingency Planning Program	Ongoing	2023
Improve Physical and Environmental Security Program Documentation	Ongoing	2023
Improve Controls over Terminated Employees	Ongoing	2020
Conduct Information Technology Security Audits	Ongoing	2022

* A status of **Complete** indicates adequate corrective action taken by management. A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

VIRGINIA MILITARY INSTITUTE

LEXINGTON, VIRGINIA 24450-0304

Finance and Budget
Office: 540-464-7270
Fax: 540-464-7794

14 August 2024

Staci Henshaw, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Henshaw:

The Virginia Military Institute has reviewed the findings and recommendations provided by the Auditor of Public Accounts for fiscal year ended June 30, 2023.

Management agrees with all findings, and we have immediately commenced the formulation and implementation of remediation.

If you have any questions or need additional information, please do not hesitate to contact me by phone at (540) 464 -7216 or by email at brownps@vmi.edu

Most Respectfully,

Pamela S. Brown
Assistant Director of Finance and Budget, Virginia Military Institute