VIRGINIA MILITARY INSTITUTE

LEXINGTON, VIRGINIA 24450-0304

Department of Information Technology
Phone 540-464-7341
Fax 540-464-7222

02 September 2024

MEMORANDUM

TO: The Audit, Finance and Planning Committee

FROM: Darrell Campbell

SUBJECT: Information Technology Report

- Security

  - Security Assessment: VMI had received a management point for not completing a "yellow book" audit of our sensitive systems by an external vendor as required by Commonwealth of Virginia IT security policies SEC502-Audit Standard in May 2023. VMI hired the BakerTilly audit firm, and the audit was completed in July 2024. However, the APA issued a new management point (tagged as recurring) because the audit was not complete by the January 2024 timeframe when the most recent APA audit cycle started.

  - The APA also issued a management point in May 2023 regarding documentation of our Windows Operating system that support the systems VMI has deemed sensitive. VMI IT has completed this task of working on furthering the documentation of system hardening to meet the APA expectations. This has been covered as part of the current APA cycle and included in the external audit. The management point was marked as closed during the last audit cycle.

  - The APA started their latest annual IT audit on the week of 1/8/24 and initially covered the two management points received in 2023. The scope was expanded to include our "Change Management" system, "Continuity of Operations", "Business Impact Analysis" and "Risk Assessment" documentation.

    Out of the most recent audit cycle VMI IT received the following management points:

    1.) VMI IT did not have the external audit of its sensitive systems performed within the specified timeframe. This was listed as a recurring management point. This audit has been performed and closed out by BakerTilly agency. They noted 27 items that will require to be resolved (or taken exception to) to meet the new SEC 530 standard. VMI IT is currently prioritizing the list of items for completion. The management point should be considered completed. The SEC

502 requirement is to have an external audit performed within every three years of our on-premise sensitive systems. VMI IT can currently expect to do this again prior to July 2027.

2.) The second point stated VMI did not conduct an effective test of its COOP. VMI also did not conduct the annual review of its Risk Management and Contingency Plan and the COOP did not include contingency procedures for one of its three MEFs (Mission Essential Functions). VMI IT has worked with the Operations and Planning office and Director of Emergency Management to ensure these items were addressed. There should be no expected reoccurrence of this MP.

3.) The third point stated VMI IT should improve physical security by documenting our review of the facility access and review physical access logs. Our ISO is now working with our Physical Plant locksmith and comparing their electronic lock system data with our server room sign in sheet monthly. He then documents he did this by updating his audit sheet. There should be no reoccurrence of this MP

- The Inspector General notified VMI of a Cyber-Security Audit (of all state public higher ed institutions). The audit for VMI started on 12/18/23 by reviewing our automated Taegis XDR monitoring system. IT also submitted other monitoring and security documentation during January 2024. IT worked with our attorney on the Rules of Engagement (ROE) documentation submitted by the OSIG auditor. The ROE represented the agreement for the penetration and security/vulnerability tests of our external facing sensitive systems. This document was signed and submitted to the OSIG auditor. At the time this report was written, VMI IT has not received a final report. Overall the OSIG group was great to work with and we received multiple collaborative communications of items they desired to see changed if possible. These items included sending Router logs, IIS logs and database logs to our XDR. These recommendations have been implemented and should meet their expectations. During the Cyber Penetration testing portion of the audit, VMI IT had one vulnerability that was immediately resolved. However, there are three issues they documented involving servers outside of IT direct support. These servers are supported by the Preston Library staff. One of the servers is on a hosted platform and the other two currently reside locally outside of IT purview. The library staff worked with the hosted partner to resolve one of the issues. IT has worked with library personnel to have the other servers updated and will be taking over patch management of the OS software of these new servers. Library personnel will still be responsible for keeping other locally installed software updated. Library personnel will also be responsible in working with the OSIG staff in satisfying the audit findings. These upgrades are expected to be completed prior to October 01, 2024.

- Vulnerability scanning: IT recently procured new software "**Tenable Vulnerability Management**" for use conducting vulnerability scanning replacing our previous "**Beyond Security**" product. This software provides the ability to scan for vulnerabilities on servers and network infrastructure by performing external and internal authenticated scans. The scan produces reports based on various security policy testing to meet PCI

"Payment Card Industry" and CIS "Center for Internet Standards" requirements and seems to be doing a very thorough job.

- PCI Assessment and attestation: FAS and IT staff in collaboration with our contractor, Campus Guard, are reviewing necessary changes to suit the new 4.0 version required for our next attestation. In September 2024, VMI IT worked with our contractor for required annual penetration testing for the PCI related Colleague system. The system was found to have three low risk vulnerabilities for IIS headers and available encryption standards. These were corrected and we are now listed as passed. VMI will need to attest in October to the new PCI 4.0 standard.

- VMI has signed a contract to have one of its on-premise sensitive system moved to the vendor's cloud infrastructure. The document imaging system "**Softdocs**" VMI currently uses in various departments and internal routable forms across Post will be relocated to their AWS cloud system which will provide multiple benefits. The change should help protect one of VMI's critical sensitive systems from potential ransom ware and VMI will ultimately utilize their security practices to protect our data. This will alleviate the three-year external SEC-502 audit requirements of this system and will also make support of the product simpler. The migration project kicked off the last week of August and is currently requested to be completed by the January 2025 timeframe if not sooner.

- VMI IT is considering changing the documented security standard it follows. VMI currently follows the State of Virgina security policy "SEC-530". VMI IT is strongly considering changes to follow the NIST 800-53 standard as most other public higher education schools that have achieved level 2 or level 3 autonomy status. This will put VMI more in align with the other public higher ed schools. VMI is currently working with Baker Tilly to determine the current security changes necessary to successfully make this change.

- Operations and Equipment

  - VMI has signed a contract with a new vendor - **OFFIX** to replace its almost 7-year-old printer fleet. The change will be replacing it current vendor- Virginia Business Systems. The printer brand will be changing from Xerox/Lexmark to Kyocera/Cannon. This will be a 5-year contract with extensions available and this change is expected to provide an annual savings in direct monthly cost and click charges compared to our current vendor. This full migration is expected to be completed by September 30, 2024.

- IT Staff Update

  VMI IT had significant turnover in July 2023 but has now become staffed at the level it was prior to our employee departures. The open Programmer position has just recently been filled. This opening was created when our internal employee promotion to fulfill our ERP DBA position happened earlier this year. We were

fortunate to fill this position with a candidate that has experience in Financial Aid and our current ERP system.

- Services

  - SharePoint Intranet Portal: Migration to the Microsoft 365 SharePoint On-line from our on-premise farm was completed by the end of June 2024. The intranet portal now has a significant updated look and feel that will hopefully be more user friendly than our previous portal.

  - Scheduling software: The Institute procured CollegeNET software for overall Post scheduling. This software will integrate easily with the Institute's Colleague ERP system as they are a direct Ellucian partner. This software should greatly enhance the efficiency of scheduling general rooms and classrooms and eventually events across the Post. This Post wide project integrating Communications & Marketing, Physical Plant and Academic departments for scheduling needs has gone well. Accuracy of the Colleague room data will be crucial to the project's success. This data in Colleague is currently being reviewed for accuracy and completeness as part of the implementation process. The goal for VMI is to have classrooms scheduled in October for the Spring 2025 term using the new software. Events and general rooms will follow shortly afterwards. The Operations and Planning department are currently backfilling from our legacy calendars into CollegeNET in preparation for going live with the overall Post implementation. Training and how-to document creation for the product has been on going as well. Operations and Planning department has the lead on the overall project with integration support provided by IT and all involved have done a magnificent job. The overall implementation project should be complete by January 2025.