


VIRGINIA INFORMATION TECHNOLOGIES AGENCY

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2025

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

AUDIT SUMMARY

We audited the Virginia Information Technologies Agency's (VITA) contract management, contract payment, centralized information technology security audit service, and right-to-use asset accounting business cycles for the fiscal year ended June 30, 2025. We found:

- proper recording and reporting of right-to-use assets, in all material respects, in the Commonwealth's lease accounting system and the Department of Accounts' (Accounts) Internal Service Fund Attachment;

- three matters involving internal control and its operation requiring management's attention, two of which also represent instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses; and

- adequate corrective action with respect to the prior audit finding identified as complete in the Findings Summary included in Appendix A.

This report also includes a Schedule of VITA-Related Risk Alerts in Appendix B applicable to multiple agencies that require the action and cooperation of VITA. Our separate audit report for each agency includes the details of each risk that we identified.

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 audit 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 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 Identifying, Tracking, Recording, and Reporting Right-to-Use Assets
Type: Internal Control
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

While the Virginia Information Technologies Agency's (VITA) Finance Department has made progress in addressing the internal control issues noted in prior audits related to right-to-use assets, it continues to lack sufficient financial reporting knowledge and resources related to Governmental Accounting Standards Board (GASB) Statements No. 87 and 96 to ensure proper identification and reporting of leases and subscription-based information technology arrangements (SBITAs). Application of these accounting standards is necessary in compiling the financial activity of VITA's internal service fund for submission to the Department of Accounts (Accounts) through a financial statement template for inclusion in the Commonwealth's Annual Comprehensive Financial Report (ACFR).

During fiscal year 2025, the Finance Department used an outside consulting firm to continue developing policies and procedures to review and monitor new and existing contracts, to record leases and SBITAs in the Commonwealth's lease accounting system, and to collect and report financial information in VITA's internal service fund financial statement template. VITA did not finalize these policies and procedures prior to fiscal year end and the compilation of the financial statement template. The Finance Department experienced a significant amount of turnover in key finance positions during the two previous fiscal years. VITA filled vacant positions and newly created positions during fiscal year 2025 to provide more resources within the Finance Department. While VITA filled positions during the fiscal year, delays in staffing key financial positions resulted in the inability to train and transition responsibilities prior to financial statement template preparation resulting in the issues noted below.

- The Finance Department incorrectly assumed that the exemption provided the year of implementation for entering contracts into the Commonwealth's lease accounting system had remained in place for the current fiscal year. Upon recognizing the error, the Finance Department had a condensed entry period for ensuring accurate and complete reporting within the Commonwealth's lease accounting system.

- The Finance Department did not adequately document evidence of evaluating, monitoring, and reviewing contracts for leases and SBITAs in accordance with its written policies and procedures.

- The Finance Department inaccurately entered lease elements within the Commonwealth's lease accounting system, resulting in misstatements for long-term and short-term SBITAs.

- The Finance Department improperly valued short-term SBITAs, resulting in a $4.1 million understatement of short-term SBITAs and affecting off balance sheet reporting in the submission to Accounts.

- The original internal service financial statement template that the Finance Department submitted to Accounts was inaccurate and incomplete. Accounts provided the Finance Department financial reporting guidance through several iterations of the template to enable the Finance Department to submit a complete and materially accurate template after its original due date. Several items reported within the template underwent revisions between the original and final submission.

Management is responsible for designing, implementing, and maintaining internal controls relevant to the preparation and fair presentation of financial information that is free from material misstatement, whether due to fraud or error. GASB Statements No. 87 and 96 prescribe the applicable accounting standards for proper accounting and financial reporting for leases and SBITAs. CAPP Manual Topics 31205 through 31220 require all agencies to follow guidelines as required by GASB Statements No. 87 and 96, and Commonwealth lease accounting system users to review the specific requirements of those statements. Generally accepted accounting principles prescribe the accounting standards for reporting internal service fund activity in the financial statement template submitted to Accounts.

While VITA made improvements from the previous year, the Finance Department should continue working to develop and implement updated policies and procedures to evaluate its contracts for potential leases and SBITAs, document adequate details of the evaluation process supporting VITA's determinations, and record leases and SBITAs correctly in the Commonwealth's lease accounting system. Management should ensure the Finance Department has adequate personnel responsible for evaluating, tracking, recording, and reporting leases and SBITAs who have the proper training and resources for accurate, complete, and timely reporting of leases and SBITAs in the Commonwealth's lease accounting system. The Finance Department should continue to develop and implement detailed policies and procedures over the compilation of VITA's internal service fund financial activity for submission to Accounts to ensure timely and accurate reporting in the future. If the Finance Department needs assistance in these areas, it should work with Accounts prior to its submission deadlines.

Continue to Ensure ITISP Suppliers Meet All Contractual Requirements

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2020

As in the prior year, VITA is not enforcing the contractual requirements for the Information Technology Infrastructure Services Program (ITISP) suppliers. VITA implemented a new service level agreement related to security patching and vulnerability management in fiscal year 2023, officially reporting and enforcing the necessary credits for the service level in June 2023 through September 2024. The requirements of this service level agreement include a Common Vulnerabilities and Exposures (CVE)

threshold, which requires that ITISP suppliers install patches with CVE scores above certain thresholds within specific time periods. If the supplier does not meet the service level time period, VITA can enforce a credit for the Commonwealth. However, for some ITISP suppliers, VITA chose not to enforce service level threshold time periods and did not request credits beginning in October 2024 through November 2025. VITA has agency-specific documented and approved policies and procedures outlining a consistent process for monitoring, adjusting, and enforcing its service level agreements with the ITISP suppliers, which do not align with the Information Technology Contracts Manual. VITA's management made the decision, based on its documented policies and procedures, not to enforce its service level agreement in accordance with the executed contracts, despite the Information Technology Contracts Manual requirement for VITA to evaluate and measure ITISP suppliers against the criteria established within the executed contract.

Our audits at various agencies for fiscal year 2025 found critical and highly important security patches not installed within 30 days as required by the Commonwealth's Information Security Standard, SEC530 (Security Standard). As a result, the systems missing critical security updates are at an increased risk of cyberattack, exploitation, and data breach by malicious parties.

The Security Standard is a baseline for information security and risk management activities for Commonwealth agencies. Many agencies rely on services provided through ITISP suppliers to ensure compliance with the Security Standard. For example, the Security Standard requires the installation of security-relevant software and firmware updates within at least 30 days of the update's release or within a timeframe approved by Commonwealth Security and Risk Management (CSRM). Commonwealth agencies rely on the ITISP suppliers for the installation of security patches in systems that support agencies' operations. When ITISP suppliers do not meet all contractual requirements (e.g., Service Level Agreements, Critical Deliverables, etc.) it impacts the ability of Commonwealth agencies that rely on the ITISP services to comply with the Security Standard.

The ITISP suppliers have struggled to mitigate vulnerabilities timely since VITA's March 2024 Security Standard revision reduced the time to apply security patches to mitigate vulnerabilities from 90 days to 30 days. VITA is responsible for reviewing and updating the Security Standard as needed; however, VITA did not perform data analysis or other research prior to establishing the 30-day threshold to ensure it was a reasonable threshold that was attainable by agencies and ITISP suppliers.

In addition, VITA continues to manage its security and event management (SIEM) tool for agencies to access, which currently stores audit logs for the ITISP infrastructure components. However, our audits of various agencies for fiscal year 2025 found that the SIEM tool does not present the information in a usable format that will allow agencies to adequately monitor their IT environments. Additionally, VITA does not configure the SIEM tool to give alerts about specific events captured in the audit logs, which are necessary to provide agencies with timely notification of potentially anomalous or malicious activity.

The Security Standard requires agencies to review and analyze audit records at least every 30 days for indications of inappropriate or unusual activity. The inability for each agency to effectively review

and monitor its audit logs increases the risk associated with the Commonwealth's data confidentiality, integrity, and availability. VITA's SIEM tool does not properly assign some audit log data to the agencies' individual dashboards, delaying agencies review and monitoring activities within their IT environments. Additionally, due to limited staffing, VITA is prioritizing its focus on correcting the audit log display before it assists agencies with configuring automatic alerts for specific audit events.

To ensure all agencies relying on the ITISP's services comply with the Security Standard, VITA should enforce supplier contractual requirements (e.g., Service Level Agreements, Critical Deliverables, etc.). If VITA determines suppliers are not meeting these requirements, VITA should implement escalation procedures to compel the ITISP services to comply with the contractual requirements. VITA should consistently enforce existing contractual requirements while conducting negotiations to modify or adjust elements of service level agreements. VITA should also analyze the Security Standard's 30-day threshold for remediating critical and high vulnerabilities to determine whether it is the appropriate threshold and feasible for ITISP suppliers and agencies to meet. In the interim, VITA should communicate with affected agencies and provide guidance on what actions the agencies can take to comply with the Security Standard while the suppliers work to meet the requirements of the contract. VITA should also continue working with the ITISP suppliers and agencies to import and configure audit log information for the SIEM tool in a usable format to ensure agencies can review the activities occurring in their IT environments in accordance with the Security Standard. Additionally, VITA should work with agencies to configure alerts for specific events captured in the audit logs to ensure agencies can detect and investigate potential malicious activity in a timely manner.

Conduct Audits of Agency Sensitive Systems Timely
Type: Internal Control and Compliance
Severity: Significant Deficiency

VITA's Centralized Information Technology Security Audit Service Department (Audit Services) conducts IT security audits for contracted agencies. The Commonwealth's Information Technology Security Audit Standard, SEC502 (Security Audit Standard) requires agencies to complete security audits for sensitive systems at least once every three years from the last audit completion date. Based on our review of audit completion dates that Audit Services provided, we determined the following:

- During fiscal year 2025, Audit Services completed three of seven (43%) agency IT security audits after the three-year audit deadline; and

- As of June 30, 2025, Audit Services was currently engaged, or had not started, five agency IT security audits that were past the three-year audit requirement.

According to Audit Services, agency requested postponements or delays caused one late audit during fiscal year 2025 and four late audits as of June 30, 2025; however, Audit Services could not provide adequate support to substantiate all agency requested postponements or agency delays. For the

remaining three audits, Audit Services did not complete the audits timely due to a shortage of resources required to complete the audits within the required timeframe.

When an agency contracts with Audit Services, the agency head or designee signs a Memorandum of Understanding (MOU) which outlines the scope of work and pricing. It is the agency's responsibility to ensure the MOU includes all sensitive systems requiring a security audit. A properly defined MOU allows Audit Services to properly price and schedule the security audits. Audit Services audits all systems in scope for an agency at the same time and issues one audit report covering all systems in scope per the MOU. Without modifications to the MOU or adequate documentation for requested delays, Audit Services is responsible for completing audits in accordance with the original MOU and SEC502.

During fiscal year 2025, Audit Services evaluated its audit work plan and staffing levels. However, Audit Services should continue to regularly monitor its audit work plan to ensure that adequate resources are available for audit staff to complete the audits by the required deadlines. For instances in which the contracting agency requests delays, Audit Services should define policies and procedure requirements for obtaining any necessary modifications or confirmations from contracting agencies and adequately document agency requested postponements or agency-caused delays. Additionally, Audit Services should assess whether VITA should contract with an outside firm to aid in completing IT security audits.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Margaret "Lyn" McDermid
Secretary of Administration

Robert Osmond
Chief Information Officer
Virginia Information Technologies Agency

We have audited the contract management, contract payment, centralized information technology security audit service, and right-to-use asset accounting business cycles of the **Virginia Information Technologies Agency** (VITA) for the year ended June 30, 2025. We conducted this 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, in support of the Commonwealth's Annual Comprehensive Financial Report audit. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objectives were to evaluate the adequacy of VITA's internal controls over contract management, contract payment, and the centralized information technology security audit service, and to evaluate the internal controls and accuracy of VITA's financial reporting related to right-to-use assets recorded and reported in the Commonwealth's lease accounting system and attachments submitted to the Department of Accounts (Accounts) for inclusion in the Annual Comprehensive Financial Report for the Commonwealth of Virginia for the year ended June 30, 2025. In support of these objectives, we also tested for compliance with applicable laws, regulations, and contract agreements and reviewed corrective actions with respect to audit findings from the prior year report. Additionally, we evaluated the accuracy of reported right-to-use assets in the Commonwealth's lease accounting system and attachments submitted to Accounts.

Audit Scope and Methodology

VITA's management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts, and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles:

Contract management
Contract payment
Centralized information technology security audit service
Right-to-use asset accounting

We performed audit tests to determine whether VITA's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of VITA's operations. We performed analytical procedures and tested details of transactions to achieve our audit objectives.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and, when appropriate, we projected our results to the population.

Our consideration of internal control over financial reporting (internal control) was for the limited purpose described in the section "Audit Objectives" 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. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve Controls Over Identifying, Tracking, Recording, and Reporting Right-to-Use Assets," "Continue to Ensure ITISP Suppliers Meet All Contractual Requirements," and "Conduct Audits of Agency Sensitive Systems Timely," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be 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. 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.

Conclusions

We found that VITA properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's lease accounting system and attachments submitted to Accounts.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management's attention and corrective action. These matters are described in the section titled "Internal Control and Compliance Findings and Recommendations."

VITA has taken adequate corrective action with respect to the prior audit finding identified as complete in the Findings Summary included in the Appendix.

Since the findings noted above include those that have been identified as significant deficiencies, they will be reported as such in the "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards," which is included in the Commonwealth of Virginia's Single Audit Report for the year ended June 30, 2025. The Single Audit Report will be available at www.apa.virginia.gov in February 2026.

Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on January 20, 2026. Government Auditing Standards require the auditor to perform limited procedures on VITA's response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response". VITA's response was not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the response.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JJR/vks

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	Fiscal Year First Reported
Improve Oversight of Third-Party IT Service Providers	Complete	2023
Improve Controls Over Identifying, Tracking, Recording, and Reporting Right-to-Use Assets	Ongoing	2022
Continue to Ensure ITISP Suppliers Meet All Contractual Requirements	Ongoing	2020
Conduct Audits of Agency Sensitive Systems Timely	Ongoing	2025

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

SCHEDULE OF VITA-RELATED RISK ALERTS

The following chart contains agencies included in our audit scope for fiscal year 2025 and impacted by the finding titled "Continue to Ensure ITISP Suppliers Meet all Contractual Requirements." These findings also impact other agencies that rely on VITA's services, which we did not include in our audit scope for fiscal year 2025.

Agency	Report Title	Issued	Risk Alert Title(s)
Department of Accounts	Department of Accounts for the year ended June 30, 2025	February 2026	Access to Centralized Audit Log Information
Department of Behavioral Health and Developmental Services	Department of Behavioral Health and Developmental Services for the year ended June 30, 2025	January 2026	Access to Centralized Audit Log Information
Department of Health	Department of Health for the year ended June 30, 2025	February 2026	Unpatched Software
Department of Medical Assistance Services	Department of Medical Assistance Services for the year ended June 30, 2025	January 2026	Access to Centralized Audit Log Information Unpatched Software
Department of Motor Vehicles	Department of Motor Vehicles for the year ended June 30, 2025	February 2026	Unpatched Software
Department of Planning and Budget	Department of Planning and Budget for the year ended June 30, 2025	February 2026	Access to Centralized Audit Log Information Timely Security Audits
Department of Taxation	Department of Taxation for the year ended June 30, 2025	February 2026	Unpatched Software
Department of Treasury	Department of Treasury for the year ended June 30, 2025	February 2026	Access to Centralized Audit Log Information

COMMONWEALTH of VIRGINIA

Robert Osmond
Chief Information Officer
Email: cio@vita.virginia.gov

Virginia Information Technologies Agency
7325 Beaufont Springs Drive
Richmond, Virginia 23225
(804) 510-7300

TDD VOICE -TEL. NO.
711

February 4, 2026

BY EMAIL

Ms. Staci Henshaw
Auditor of Public Accounts (APA)
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

The Virginia Information Technologies Agency (VITA) appreciates the opportunity to respond to the combined audit of VITA's contract management, contract payment, centralized information technology security audit service, and right-to-use asset accounting business cycles covering the fiscal year that ended on June 30, 2025. We commend the time, effort, and professionalism of your staff in completing the assessment and report.

The report identifies three audit findings, as well as one completed finding. This response letter addresses each of the open findings, explains our understanding of the findings, and the actions we plan to take to remediate.

Finding Title: Improve Controls Over Identifying, Tracking, Recording, and Reporting Right-to-Use Assets

VITA acknowledges the audit finding and agrees that, while improvements have been made in addressing internal control issues related to right-to-use assets, additional corrective actions are necessary to ensure full compliance with Governmental Accounting Standards (GASB) Statements No. 87 and No. 96.

VITA incorrectly assumed that the availability of the bulk submission functionality in the Commonwealth's lease accounting system existed, as in previous years. Given the massive amount of data that needed to be entered, VITA built its process for entering contracts around this functionality. Once VITA learned that the bulk submission functionality was unavailable with the Commonwealth's lease accounting system, VITA immediately initiated a manual process to enter leases and SBITAs in the Commonwealth's lease accounting system. It is important to note the following: (1) VITA did not wait until the data was entered into the Commonwealth's lease accounting system to review the lease or right to use obligations, with an implication that VITA's outstanding responsibility was just data entry into the Commonwealth's

lease accounting system; and (2) any delay in entering the data into the Commonwealth's lease accounting system did not impact the accurate and complete reporting of information in the Commonwealth's lease accounting system and, ultimately, the ACFR. Going forward, VITA will obtain formal documentation whenever the Department of Accounts grants VITA an exception to a policy or procedure. In addition, management will refine VITA's policies and procedures over the lease asset process to ensure VITA has properly captured all leases and entered all lease data in the Commonwealth's lease accounting system. The finalized procedures will include a step to verify and update processes for relevant changes that have occurred during the year that may have an impact on VITA's year-end financial reporting.

The finding also states that VITA did not adequately document evidence of evaluating, monitoring, and reviewing contracts for leases and SBITAs. While VITA acknowledges that documentation supporting the evaluation, monitoring, and review of lease contracts was not consistently maintained, VITA did, in fact, perform the required review. To increase efficiency and effectiveness, policies and procedures were initially drafted by VITA, with the understanding that VITA would continue to refine processes while taking into consideration the complexity of VITA's operating model. Also, VITA drafted an exception statement that documented the exceptions taken that were not part of the written policies and procedures. These steps were taken to limit the amount of time and constraints on VITA's staff due to the manual nature of this work and the volume of service contracts that VITA maintains. VITA will secure additional training for all finance department staff regarding the implementation of GASB Statements No. 87 and No. 96, including detailed guidance on lease identification, classification, valuation, and disclosure requirements.

VITA appreciates the APA's recognition that VITA has made progress in addressing the internal control issues related to right-to-use assets, as evidenced by APA categorizing this finding as a significant deficiency in the current audit (as opposed to a material weakness as documented in the fiscal year 2024 audit). VITA appreciates the insights and recommendations provided by the APA and remains committed to maintaining and enhancing the integrity of our financial reporting.

Finding Title: Continue to Ensure ITISP Suppliers Meet All Contractual Requirements

VITA concurs with APA's findings and recognizes the opportunity to continuously improve. VITA has a security standard (SEC530), and the APA is correct in pointing out that audits at various agencies for fiscal year 2025 revealed some critical and high security patches were not installed within 30 days as required by the Commonwealth's Information Security Standard (SEC530). VITA also appreciates the acknowledgement that VITA has documented and approved policies and procedures outlining a consistent process for monitoring, adjusting, and enforcing its service level agreements (SLAs) with the ITISP suppliers. Using APA's prior-year feedback, VITA substantially improved our documented processes and operational activities.

VITA's internal analysis of our vulnerability management program indicates that 84% of critical and high vulnerabilities are remediated within the 30-day standard which means that 16% do not meet the standard. Although a substantial improvement, we agree that more is needed. The

Commonwealth's information technology environment operates in a decentralized manner with VITA responsible for enterprise infrastructure and cybersecurity and agencies responsible for agency applications and data assets (with personnel and funding being allocated by the General Assembly in support of this model). Although there is an apparent clear delineation of responsibility, security patches often have broad impacts on both the infrastructure and the applications. In many cases, security patches intended to address critical and high vulnerabilities would result in breaking agency applications and must be deferred until the agency can modernize their applications such that the security patch can be accepted. When agencies were unable to accept the security patch, VITA waived the supplier's responsibility to deploy the security patch. VITA needs to improve our teamwork and collaboration between VITA staff, our suppliers, and agency customers.

VITA has also more aggressively enforced change freezes in the VITA operational environment to protect critical functions including emergency management during emergency events (such as winter weather snow events, flooding, and hurricanes), holidays, and elections. 2025 was a very busy year for elections (which included 45 days of early voting) with a total of seven elections (general, primary, and special elections) occurring during the year. During emergency events, holidays, and elections, VITA applies a change freeze that prevents the deployment of patches, so VITA suppliers are not held responsible for delays that occur due to Commonwealth direction. VITA has determined that the operational readiness of our applications during emergency events, the minimization of risks during holidays when staff are not available, and maintaining the high integrity of our election process outweigh the VITA standard. VITA agrees with the APA that documentation of such deferrals (including the impact on deferred patching) is not done at a detailed enough level to provide better supplier accountability.

As we improve our vulnerability and supplier management capabilities, we are also improving our comprehensive cybersecurity capabilities as part of our Zero Trust initiative. Over the last four years, VITA has increased compensating controls and measures at the enterprise infrastructure level, including our security information and event management (SIEM) software, our improved vulnerability scanning and intrusion detection tools, our improved vulnerability and risk visualization tool, our improved website security tool, and our data loss prevention tools. We have also upgraded our identity management and multi-factor authentication tools to better secure user identity. All these tools and capabilities provide additional compensating security measures that prevent threat actors from gaining access to the servers and services where potential exploitation of a vulnerability could occur.

VITA thanks the APA for their analysis, insight and advice. We strive to improve and look forward to our continued partnership with APA to improve cybersecurity and serve our joint customers better.

Finding Title: Conduct Audits of Agency Sensitive Systems Timely

VITA acknowledges the observation of the APA that certain audits of agency sensitive systems were not completed within the prescribed timeframes. However, VITA respectfully asserts that the characterization of the delays does not fully reflect the underlying causes or the respective

responsibilities of the parties involved. Each agency is responsible for completing security audits in accordance with the Commonwealth's Information Technology Security Audit Standard, SEC502. Similar to APA, and as outlined in MOUs, the VITA Cybersecurity Audit Service relies on our customer agencies providing supporting information and assistance on a timely basis. When that does not happen, audit completions are delayed. This happened in several of the eight late occurrences identified. In FY2025, VITA's Audit Services team performed seven audits. Four audits were completed timely within the planned period of performance. Three agency IT security audits were completed but after the three-year audit deadline during FY 2025, and five agency IT audits were delayed past the three-year audit requirement as of June 30, 2025. Of the five delayed agency IT audits, one was completed as of December 30, 2025, and the other four were postponed by the agency.

Although VITA knowledges that the Audit Services Department's staffing may have played a role, it was not the primary root cause for audits not being completed on a timely basis. During fiscal year 2025, VITA's Audit Services Department performed an evaluation of its audit workplan and staffing levels. Although staffing levels are limited to the current Maximum Employment Level (MEL) count, and cybersecurity vacancies remain difficult to fill, VITA's Audit Services Department continues to leanly and efficiently deliver. VITA's leadership routinely evaluates its workplan and staffing levels (including the use of contractors and vendors) to ensure adequate resources are available for audit staff to complete IT security audits by the required deadlines, while also balancing the cost of the program to agencies that are fiscally challenged. In the future, to improve the efficiency and effectiveness of the Audit Service program, VITA intends to provide a more detailed work plan to the agencies being audited to more clearly establish information that needs to be provided to VITA to enable VITA to deliver the planned audits on a timely basis.

Thank you again for your staff's work, insight, and commitment to our success, and we look forward to working with you in the future.

Sincerely,

Robert Osmond

cc (by email) Secretary of Administration Traci J. Deshazor