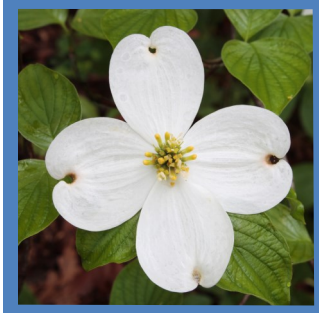

VIRGINIA INFORMATION TECHNOLOGIES AGENCY

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2024

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, 2024. 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, after adjustment for the misstatements noted in the finding "Improve Controls Over Identifying, Tracking, Recording, and Reporting Right-to-Use Assets;"

- three prior audit matters involving internal control and its operation necessary to bring to management's attention, one of which is considered a material weakness, where corrective action is ongoing as shown in the Findings Summary included in the Appendix; and

- two instances of noncompliance with applicable laws and regulations or other matters that are required to be reported.

This report also includes an appendix of Risk Alerts 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 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 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.

VITA is one of several entities cited in a risk alert in Accounts fiscal year 2024 audit report. The "Financial Reporting" risk alert identifies the increased risk that the Commonwealth may not meet the deadline for the Annual Comprehensive Financial Report, which could jeopardize the Commonwealth's bond rating, because multiple entities have increasingly submitted inaccurate and late financial information to Accounts over the past several fiscal years. As an entity that is contributing to this increased risk for the Commonwealth, VITA's corrective action to correct the issues in the finding "Improve Controls Over Identifying, Tracking, Recording, and Reporting Right-to-Use Assets" is essential to reducing the risk to the Commonwealth.

-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: Material Weakness
First Reported: Fiscal Year 2022

The Virginia Information Technology Agency's (VITA) Finance Department continues to lack sufficient financial reporting knowledge and resources to ensure proper identification and reporting of leases and subscription-based information technology assets (SBITAs) and apply the applicable accounting standards in compiling and submitting VITA's internal service fund activity timely to the Department of Accounts (Accounts) for inclusion in the Commonwealth's Annual Comprehensive Financial Report (ACFR). VITA's Finance Department made progress in addressing issues identified in prior years related to the evaluation of its material contracts to determine whether the contracts qualified for reporting as leases or SBITAs by hiring an outside consulting firm that created a position paper on each material contract documenting VITA's philosophy on how to classify purchases under each contract. However, the Finance Department did not adequately correct recorded lease and SBITA information in the Commonwealth's lease accounting system to address misstatements and inaccuracies that resulted in audit adjustments in fiscal year 2023.

During fiscal year 2024, the Finance Department did not have sufficiently updated policies and procedures to meet the complexity of VITA's business operations 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 Attachment. The Finance Department used an outside consulting firm to develop policies and procedures for these areas; however, the policies and procedures did not adequately address the complexity of VITA's business operations. In addition, the Finance Department did not follow these policies and procedures during fiscal year 2024 or while compiling the Internal Service Fund Attachment after fiscal year end. The Finance Department experienced a significant amount of turnover in key finance positions for the second consecutive year. Difficulty in recruiting and retaining qualified staff has created a knowledge gap in key financial positions, which compounded the lack of adequate policies and procedures resulting in the issues noted below.

- The Finance Department did not adequately document its evaluation of contracts, other than the material contracts noted above, to determine whether the purchases under each contract qualified for reporting as leases or SBITAs.

- The Finance Department did not review or verify the new lease and SBITA information that Accounts uploaded for VITA in the Commonwealth's lease accounting system to ensure the information was reasonable and accurate.

- The Finance Department did not correct recording errors noted in the fiscal year 2023 audit related to leases and SBITAs, which affected the reporting of leases and SBITAs in VITA's Internal Service Fund Attachment for fiscal year 2024.

- The Finance Department interpreted purchase order descriptions incorrectly and improperly valued short-term SBITAs, which resulted in a $23.7 million overstatement of short-term SBITAs, reported to Accounts for off balance sheet reporting.

- The original Internal Service Fund Attachment that the Finance Department submitted to Accounts was materially inaccurate, incomplete, and unusable. Accounts provided the Finance Department financial reporting guidance through several iterations of the Attachment to enable the Finance Department to complete a materially accurate submission 77 days after its original due date. Almost every line item on the Internal Service Fund Attachment changed between the original and final submission by amounts ranging from $4,611 to $115.5 million.

- The Finance Department applied incorrect discount rates to 15 of 15 (100%) SBITAs tested, and in 6 of the 15, the value of the SBITA was above the $2 million threshold for application set out in Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 31305.

In addition to the specific misstatements noted above, these issues resulted in misstatements ranging from $15,043 to $91.1 million for the various lease and SBITA-related financial statement line items, including intangible right-to-use capital assets, long-term liabilities, amortization, rent, and interest expense, as well as the associated footnote disclosures. Reporting incorrect amounts to Accounts in the Internal Service Fund Attachment could lead to inaccurate financial information reported in the ACFR. We consider these deficiencies in internal control to be a material weakness because the combination of issues noted create a reasonable possibility that a material misstatement of financial information will not be prevented, or detected and corrected, on a timely basis.

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. Governmental Accounting Standards Board (GASB) Statements No. 87 and 96 prescribe the applicable accounting standards surrounding the 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 the Commonwealth's lease accounting system users should review the specific requirements of those statements. Generally accepted accounting principles prescribe the accounting standards surrounding the reporting of the internal service fund activity in the Internal Service Fund Attachment submitted to Accounts.

VITA's discount rate policy that was effective for fiscal year 2024 does not comply with CAPP Manual Topic 31305. CAPP Manual Topic 31305 allows the use of the Department of Treasury's Master Equipment Lease Program (MELP) interest rates only for SBITAs that have a term less than 72 months and an asset value less than $2 million. VITA's discount rate policy applies the MELP interest rates as the incremental borrowing rate for all leases and SBITAs and uses the rate effective at the beginning of the fiscal year, regardless of SBITA start date, term, or valuation. The CAPP Manual requires using the quarterly MELP rate that is closest to the start date of the SBITA.

The Finance Department should continue working with the outside consultant to develop and implement updated policies and procedures to evaluate contracts for leases and SBITAs and document adequate details of the evaluation process to support VITA's determinations and to record leases and SBITAs 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 develop and implement detailed policies and procedures over the compilation of VITA's Internal Service Fund Attachment 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. The Finance Department should ensure its discount rate policy complies with the CAPP Manual and consistently adhere to the policy when recording leases and SBITAs.

Continue to Ensure ITISP Suppliers Meet All Contractual Requirements

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

VITA has made significant progress to monitor and enforce the contractual requirements for the Information Technology Infrastructure Services Program (ITISP) suppliers. During fiscal year 2024, VITA and the Multisource Service Integration (MSI) continued to evaluate the current service level measurements to ensure they align with the Commonwealth's needs. VITA and the MSI monitored the service level related to security and vulnerability patching for the entire fiscal year. The requirements of this service level for fiscal year 2024 included a Common Vulnerabilities and Exposures (CVE) threshold, which required that ITISP suppliers install any patch with a CVE score above the threshold within 60 days. If the supplier did not meet the service level threshold, VITA enforced a credit for the Commonwealth.

Although VITA monitored the service levels implemented in the prior year, not enough time has passed to prove the effects of the consequences enforced. Our audits at various agencies for fiscal year 2024 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. 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 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.

Additionally, during fiscal year 2024, VITA continued to work with the managed security supplier to address the inability of agencies to access the audit log information in the managed detection and response (MDR) platform. VITA implemented a separate security and event management (SIEM) tool at the end of October 2023 to expand agencies' capabilities to monitor audit log information. While the supplier implemented the MDR platform, VITA and the supplier determined to replace the MDR platform with the VITA-managed SIEM tool as the permanent audit log monitoring tool. However, while the SIEM tool is in production, it also does not include all audit log information in a usable format to allow agencies to adequately monitor their IT environments.

The Security Standard requires agencies to review and analyze audit records at least every 30 days for indications of inappropriate or unusual activity. Our audits of various agencies for fiscal year 2024 found that agencies rely on VITA and ITISP suppliers to provide access to a centralized monitoring tool that collects audit log information about activities in the IT environment. Although the supplier was performing audit logging and monitoring, most agencies were unable to obtain access to the audit log information during fiscal year 2024, and thus, were not able to comply with the Security Standard requirements related to audit log monitoring. An inability for all agencies to review and monitor their individual audit logs increases the risk associated with the Commonwealth's data confidentiality, integrity, and availability.

To ensure all agencies that rely on the ITISP's services comply with the Security Standard, VITA should ensure suppliers meet all 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. Additionally, VITA should communicate with the affected agencies and provide guidance on what the agencies can do 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 audit log information to the SIEM tool to ensure agencies can review the activities occurring in their IT environments in accordance with the Security Standard.

Improve Oversight of Third-Party IT Service Providers

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2023

VITA does not sufficiently document the timeliness and completeness of its oversight of information technology (IT) third-party service providers in accordance with CAPP Manual Topic 10305 and the Security Standard. VITA contracts with several service providers to provide IT infrastructure services. VITA obtains assurance over the operating effectiveness of the controls at each service provider by obtaining and reviewing System and Organization Controls (SOC) reports for both financial reporting (SOC 1) and IT security (SOC 2). VITA also obtains SOC reports for subservice providers when necessary. Although VITA obtained and reviewed all required SOC reports for fiscal year 2024, we identified the following weaknesses:

- for eight of eight (100 percent) service providers and key subservice providers that included complementary user entity controls (CUECs) in their SOC report, VITA did not document how the agency ensures CUECs are in place and operating effectively;

- for four of four (100 percent) service providers with exceptions to control objectives, VITA did not document how the exceptions affect VITA's operations or why the exceptions did not affect VITA's operations;

- for two of seven (29 percent) service providers with subservice organizations identified in the SOC reports, VITA did not identify the name of the subservice organization(s) within its review checklist; and

- for two of three (66 percent) subservice providers, the period of the SOC reports provided did not include the beginning of fiscal year 2024. Upon request, VITA provided one of two (50 percent) earlier SOC reports covering the beginning of fiscal year 2024; however, documentation of VITA's review was not included. VITA did not provide a SOC report covering the beginning of fiscal year 2024 for the remaining subservice provider.

The Security Standard states that the agency head of each agency is accountable for maintaining compliance with the Security Standard, and that agencies must enforce the compliance requirements through documented agreements with third-party providers and oversight of the services provided. Additionally, CAPP Manual Topic 10305 requires agencies to have adequate interaction with service providers to appropriately understand the service providers' internal control environments. Agencies must also maintain oversight over service providers to gain assurance over outsourced operations.

A primary cause of the weaknesses identified above is a lack of time to thoroughly review and document the evaluations of the SOC 1 reports. VITA expects all service providers to submit SOC 1 reports by September 1, and SOC 2 reports by November 1, of each year. When VITA receives the SOC reports, analysts review the reports and document their evaluation using the SOC Review Checklist. When there is a delay in obtaining SOC reports from service providers, there is not sufficient time to thoroughly review the reports and evaluate the results. Although VITA completed the SOC 1 Review Checklists for each service provider and subservice provider, several checklists did not contain adequate documentation of considerations related to CUECs or the effects of control objective exceptions on VITA's operations.

VITA should ensure that all staff responsible for reviewing SOC reports, and completing SOC Review Checklists, receive adequate training on the various components of SOC reports and the SOC Review Checklists to be able to thoroughly complete the checklists and evaluations. VITA should consider adding a review element to the SOC Review Checklists to ensure that all evaluations contain sufficient documentation of service provider oversight. When VITA identifies exceptions to control objectives in the SOC reports, VITA should sufficiently document the effect of those control objective exceptions on VITA and the Commonwealth. Additionally, when VITA identifies CUECs in the SOC reports, VITA should include sufficient documentation of its consideration of the CUECs.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 13, 2024

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, 2024. 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 Accounts for inclusion in the Annual Comprehensive Financial Report for the Commonwealth of Virginia for the year ended June 30, 2024. 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 and recommendations 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 the Department of Accounts (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 also 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. 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 material weaknesses 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 Identifying, Tracking, Recording, and Reporting Right-to-Use Assets," 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 "Continue to Ensure ITISP Suppliers Meet All Contractual Requirements" and "Improve Oversight of Third-Party IT Service Providers," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," to be significant deficiencies.

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, after adjustment for the misstatements noted in the finding "Improve Controls Over Identifying, Tracking, Recording, and Reporting Right-to-Use Assets."

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."

Since the findings noted above include those that have been identified as a material weakness or 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, 2024. The Single Audit Report will be available at www.apa.virginia.gov in February 2025.

Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on January 31, 2025. 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

ACS/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
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
Improve Oversight of Third-Party IT Service Providers	Ongoing	2023

* **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 2024 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 2024.

Agency	Report Title	Issued	Risk Alert Area(s)
Department of Accounts	Department of Accounts for the year ended June 30, 2024	February 2025	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, 2024	January 2025	Access to Centralized Audit Log Information Unpatched Software
Department of Health	Department of Health for the year ended June 30, 2024	February 2025	Unpatched Software
Department of Medical Assistance Services	Department of Medical Assistance Services for the year ended June 30, 2024	January 2025	Access to Centralized Audit Log Information Unpatched Software
Department of Motor Vehicles	Department of Motor Vehicles for the year ended June 30, 2024	February 2025	Unpatched Software
Department of Planning and Budget	Department of Planning and Budget for the year ended June 30, 2024	January 2025	Access to Centralized Audit Log Information
Department of Taxation	Department of Taxation for the year ended June 30, 2024	February 2025	Unpatched Software
Department of Treasury	Department of Treasury for the year ended June 30, 2024	February 2025	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 6, 2025

BY EMAIL

Ms. Staci Henshaw
The Auditor of Public Accounts

Dear Ms. Henshaw:

Thank you for the opportunity to respond to the combined audit of the Virginia IT Agency's (VITA) contract management, contract payment, and right-to-use asset accounting business cycles covering the fiscal year that ended on June 30, 2024 (FY24). We commend the time, effort, and professionalism of your staff in completing the assessment and report. We especially want to commend the APA for their help remediating the deficiencies cited to achieve our shared goal of accurate financial reporting.

The report identifies three open findings. This response letter addresses each of the open findings, explaining our understanding of the findings and the actions we plan to take.

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

The relatively new Governmental Accounting Standards Board (GASB) Statement No. 87 and Statement No. 96 ensure proper identification and reporting of leases and subscription-based information technology assets (SBITAs) and have required that VITA completely re-engineer our systems, processes, and organization for thousands of assets (and millions of transactional obligations) that VITA processes on behalf of the agencies that we serve. This is particularly relevant as the majority of software has transitioned from purchased software to subscription-based software. This finding emphasizes the state of policies and procedures for the review, monitoring, recording of new and current contracts and leases and subscription-based information technology assets (SBITAs) and recognizes that VITA (with help from DOA and the APA) had to develop our practices throughout the fiscal year. As a result of the FY23 audit, Finance memorialized and updated policies and procedures, provided training on them as newly hired staff, modified our financial system reporting tools to classify the assets properly, loaded the data into the Department of Accounts Lease Accounting System (LAS), and created new financial reports. The ongoing dynamic of both the policy and procedures documentation and

the high turnover created times during the fiscal year when Finance activities did not align with the most recent written policies and procedures. This is an area of ongoing improvement, and we have partnered with the Department of Accounts (DOA) to improve training in the spring to better support finance activities such as the Attachment 11 and activities in support of the Annual Comprehensive Financial Report (ACFR).

The finding also states that there was no evaluation of contracts to determine if they are recordable as leases or SBITAs. We interpreted certain contracts as outside the scope of SBITAs and recordable leases, but based on APA's guidance on our interpretation, we reclassified them and will apply that interpretation in future fiscal years.

The finding states that VITA incorrectly interpreted purchase order descriptions. We will align our future interpretations with APA's perspective.

Lastly, the finding characterizes VITA's discount rate policy that was effective for fiscal year 2024 as incompliant with the Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 31305. Going forward, we will apply the discount rate according to APA's clarification.

Finding Title: Improve Oversight of Third-Party IT Service Providers

We appreciate APA's attention to the important area of third-party oversight. VITA and the APA are unified in our shared goal of exemplary Commonwealth cybersecurity. In working with APA's auditing staff in FY23 and FY24, there are two primary issues that require resolution to ease audit timeline issues and clarify the requirements for VITA's review of System and Organization Controls (SOC) reports.

Because of the lack of an agency timeliness standard, the finding evaluated VITA's review of SOC reports based on APA's audit timeline, which allows only approximately 2 months from the time SOC reports are received until audit work is finished, creating challenges for both APA and VITA. VITA has a process for addressing issues found in reviews of SOC reports, but that process lacks sufficient detail to set expectations and timelines. The agency standard needs to be further revised, improved and clarified to define the agency review process and schedule more thoroughly.

To support the audit cycle engagement and aid both APA and VITA, VITA proposes that, going forward, VITA clarifies the review process (included timing), documents the process more thoroughly using SOPs, and provides APA with documentation of VITA having (i) received and reviewed SOC reports for the FY that is the subject of the audit, such as the SOC report review checklists; and (ii) acted on the prior year CUEC issue(s), such as logged Work Management Module (WMMs) (discussed below). This would show a working SOC report review and operational action program, demonstrating that prior year issues have been addressed or are not a problem and that the process has begun for the year of the audit.

VITA agrees with having accountability for resolution of CUECs and other SOC report issues. We intend to ensure that action to address CUEC and issues from SOC reports starts ASAP after review of the reports (approximately in October), with the goal of concluding whatever action is appropriate by approximately May/June (in terms of actual action taken, leaving aside further regular monitoring and review to verify the issue has been fully addressed). This would enable us to address any questions and provide supporting documentation by the close of the fiscal year. Going forward, service providers and key subservice providers that include complementary user entity controls in the SOC report, VITA will document how the agency ensures the controls are in place and operating effectively.

A second issue may exist with respect to the scope of the finding. The finding concerns VITA's review and completion of the SOC checklist and SOC reports. VITA has overall supplier and security management functions and processes to address various types of issues that arise, but those are separate from the SOC report review process. The SOC report review process concludes with completion of the checklists and then logging governance cases (WMMs) on identified issues. Those WMMs then proceed for appropriate evaluation and resolution with relevant stakeholders through VITA's overall supplier management functions and processes. To illustrate and document the process, VITA provided APA with two examples of WMM exports that document past action.

In response to this finding, VITA will work with APA to address the above issues and also will improve SOC report review documentation. Specifically, we will refine the SOC review checklist to:

- "document and reference third-party supplier management activities in the SOC report evaluation tool";
- include the "responses added by the employee completing the checklist per the checklist instructions;
- explicitly indicate any "further considerations related to each complementary user entity controls"; and
- "describe the effects of each Control Objective exceptions on VITA operations".

Finding Title: Continue to Ensure all Contractual Requirements are met by ITISP Suppliers

VITA continues to agree with APA that security compliance is an important area for ongoing assessment, and we appreciate the finding's acknowledgement that significant progress has been made. We also agree with APA that the applicable standard for assessment of patching, vulnerability scanning, and other aspects of cybersecurity is SEC530. The challenge is that the standard is intentionally progressive to drive continued improvement. For example, the prior standard was to complete vulnerability patching within 90 days. When the majority of those vulnerabilities met the standard, VITA tightened the standard to 30 days. VITA believes that

security standards compliance in a large and complex enterprise environment, along with management and adjustment of related contractual service level agreement (SLAs), is an ongoing effort in which continual improvement is sought. The finding acknowledges that SEC530 is a newer, tougher standard that became effective in 2024, and that VITA and the Commonwealth must continuously improve cybersecurity.

Vulnerability remediation is a shared responsibility between the VITA suppliers and the agencies. There are challenges with the patching standard because legacy agency applications may break, and agency business processes would be adversely impacted. Agencies are under-resourced and dealing with technical debt. In many cases, the agency application software is obsolete and deploying patches would result in agency applications becoming inoperable. The large and complex enterprise also can present challenges in scheduling patch rollouts around various critical events and efforts, both planned and unplanned. (For example, VITA institutes change freezes to avoid disruption at times of disaster and for planned critical periods such as elections.) VITA offers exceptions to address this situation.

Suppliers and VITA have proposed to agencies, through RMC and other agency engagement groups, a more aggressive patching schedule designed to improve compliance; agencies are considering that model. Agency impacts and resource and operational considerations dictate a measured approach, albeit one that works to drive cybersecurity forward on an ongoing basis. VITA does and the executive branch have had notable success in cybersecurity to date that has been recognized by third parties (for example, in cyber insurance policy rates and coverage that have gone down for a second year in a row as the external insurer acknowledges lower overall cybersecurity risk). More improvement is possible.

Security log information access is similarly an area in which ongoing work with agencies is needed. As the finding notes, VITA has rolled out centralized monitoring / logging tools and offered training to agencies. VITA Commonwealth Security and Risk Management (CSRM) has devoted resources specifically to providing additional support to agencies related to these tools, and this area is repeatedly discussed at agency engagement meetings. Identification of relevant logs and ingestion of them into the tools is an ongoing effort working with each agency.

VITA also notes that supplier performance on the patching SLA (1.1.3) has improved. During the 12 months of FY24, we had an average of 1.1 supplier defaults per month. For the five reported months of FY25 to date, there was an average of 0.6 defaults per month, a significant decrease. The two most recent months reported had no supplier defaults on patching (SLA 1.1.3), a sign trending toward even more improvement. Security and supplier performance is improving, and VITA intends to continue that progress.

Finally, VITA notes that it has been making the case to policymakers for increased investment in technology modernization and cybersecurity. Governor Youngkin's administration has been supportive, and VITA has been developing new data and ways of assessing and planning for modernization, working with the input of agencies and advice of policymakers. VITA also will continue to work with agencies on opportunities for shared services, common applications, and

other efficiencies that can help the executive branch meet the challenge of modernization (including improved cybersecurity) together.

In conclusion, thank you again for your staff's work and the insight provided by your review.

Sincerely,

Robert Osmond

cc (by email): Secretary of Administration Lyn McDermid