VIRGINIA INFORMATION TECHNOLOGIES AGENCY

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 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, 2023. 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' financial statement template, after adjustment for the misstatements noted in the finding "Improve Controls over Identifying, Tracking, Recording, and Reporting Right-to-Use Assets";

- three matters involving internal control and its operation necessary to bring to management's attention, of which, we consider one finding to be a material weakness;

- one instance of noncompliance with applicable laws and regulations or other matters that is required to be reported; and

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

This report also includes an appendix of Risk Alerts applicable to multiple agencies that requires 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 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 recommendations.

-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 Issued: Fiscal Year 2022
Prior Title: Improve Controls over Identifying, Tracking, Recording, and Reporting Leased Assets

Virginia Information Technologies Agency's (VITA) Finance Department lacked sufficient financial reporting knowledge and resources to appropriately implement Governmental Accounting Standards Board (GASB) Statement No. 87 and Statement No. 96. As a result, VITA was not able to ensure proper identification and reporting of leases and subscription-based information technology arrangements (SBITAs) and apply the applicable accounting standards in compiling the financial activity for VITA's internal service fund for submission to the Department of Accounts (Accounts) within the required timeframe for inclusion in the Commonwealth's Annual Comprehensive Financial Report (ACFR). GASB Statement No. 87 was effective in fiscal year 2022, and GASB Statement No. 96 was effective for the current fiscal year. We identified issues with VITA's implementation of GASB Statement No. 87 in the prior year audit, however, VITA did not implement sufficient corrective action to rectify the issues. The reporting under GASB Statement No. 96 mirrors GASB Statement No. 87. As a result, VITA's implementation of GASB Statement No. 96 included the same issues as in the prior year.

Due to the lack of knowledge and staffing resources, and the issues identified in the prior year audit, VITA hired an outside consulting firm to assist with evaluating some leases and SBITAs and to provide VITA's Finance Department guidance on its policies, procedures, and training on leases and SBITAs. However, the consulting firm, along with VITA management and the Finance Department, did not obtain an adequate understanding of VITA's contracts to determine whether the contracts qualified for reporting as leases or SBITAs. In addition, they did not ensure that VITA's implementation was consistent with the Commonwealth's method of implementation and the Commonwealth Accounting Policies and Procedures (CAPP) Manual requirements for recording and reporting leases and SBITAs. VITA's implementation processes were deficient in the following areas, resulting in misstatements ranging from $15,000 to $71.7 million for various 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:

- The Finance Department did not properly report SBITA beginning balances for contracts that were in effect at the beginning of the year of implementation, instead including them in current year additions. As a result, they understated the beginning balances for assets and liabilities by $71.7 million and $64.4 million, respectively.

- The Finance Department did not accurately determine or record the lease or SBITA term across all contracts. As a result, it improperly classified the largest SBITA asset, understating

the right-to-use asset and the long-term liability by $64.2 million and $29.7 million, respectively.

- The Finance Department did not properly record the lease and SBITA payments as rent expense, understating the rent expense line item by $43.9 million.

- The Finance Department did not properly identify, evaluate, or disclose variable payments of $26.1 million in leases and $18.6 million in SBITAs.

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

- The Finance Department did not identify a complete population of contracts to review. In addition, the department did not document its review of each contract, including support for its determination of whether a contract qualifies as a lease or SBITA under GASB Statement 87 or 96. The Finance Department also did not adequately evaluate all active contracts where VITA pays the vendor to ensure it included the complete population of leases and SBITAs in the Commonwealth's lease accounting system for financial reporting by the proper agency.

- The Finance Department did not implement compensating controls over billing data provided by vendors. During the fiscal year, one of VITA's major vendors received a qualified opinion related to its billing data within its system and organization controls (SOC) report. The Finance Department did not perform a reconciliation to verify and ensure the completeness and accuracy of the leased and SBITA asset data the vendor provided for use in valuing VITA's lease and SBITA assets and liabilities.

- The Finance Department did not develop sufficient lease or SBITA implementation policies and procedures to ensure consistent and reasonable evaluation across contracts, Commonwealth's lease accounting system recording, or financial reporting.

VITA maintains and manages various complex, multiple component statewide contracts containing leased assets, SBITAs, and non-lease or non-subscription components. VITA reports the financial activity related to leases and SBITAs for its internal service funds to Accounts through a financial statement template for inclusion in the Commonwealth's ACFR. GASB Statements 87 and 96 have dramatically impacted the financial reporting requirements for VITA in the last two years. VITA management and the Finance Department did not appropriately plan for and prioritize these financial reporting requirements. We consider the combination of issues noted to be a material weakness in internal control as the current process does not prevent, or detect and correct on a timely basis, material misstatements to the financial statements.

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 87 and 96 prescribe the applicable accounting standards for the proper accounting and financial reporting for leases and SBITAs. CAPP Manual Topics 31205 through 31220 state all agencies must follow guidelines as required by GASB Statements 87 and 96, and the Commonwealth's lease accounting system users should review the specific requirements of those statements.

VITA's Finance Department did not have an accurate understanding of GASB Statements 87 and 96. VITA personnel involved in gathering and evaluating lease and SBITA information did not obtain the necessary training to be able to properly plan, prepare, and implement GASB Statements 87 and 96. VITA management should prioritize the need for and importance of preparing accurate financial information in accordance with generally accepted accounting principles within the required timeframe for inclusion in the ACFR. VITA's management should ensure the individuals evaluating, tracking, recording, and reporting leases and SBITAs obtain training and the appropriate resources to ensure they have a thorough understanding of the requirements of GASB Statements 87 and 96. Management should develop, implement, and update policies and procedures regularly over VITA's lease and SBITA accounting process to ensure accurate and complete reporting. In addition, management should perform an evaluation over all VITA contracts to ensure the Finance Department has properly captured all leases and SBITAs, corrected any misstated leases or SBITAs, and entered all lease and SBITA data in the Commonwealth's lease accounting system. Furthermore, VITA should retain records of all implemented compensating and complementary controls related to billing data, such as reconciliations, to mitigate the risk of vendor information being inaccurate in comparison to the contract and payments made to vendors.

Continue to Ensure ITISP Suppliers Meet all Contractual Requirements
Type: Internal Control
Severity: Significant Deficiency
First Issued: Fiscal Year 2020

Although VITA is monitoring and enforcing the contractual requirements each month, as of June 2023, there were still cases of Information Technology Infrastructure Services Program (ITISP) suppliers not meeting the minimum requirements. When ITISP suppliers do not meet all contractual requirements (e.g., key measures, critical service levels, deliverables, etc.), it impacts the ability of Commonwealth agencies that rely on the ITISP services to comply with the Commonwealth's Information Security Standard, SEC 501 (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 updates within 90 days of release *(Security Standard, Section SI-2 Flaw Remediation)*. Commonwealth agencies rely on the ITISP suppliers for the installation of security patches in systems that support agencies' operations. Our audits at various agencies for fiscal year 2023 found critical and highly important security patches not installed within the 90-day Security Standard requirement. The systems missing critical security updates are at an increased risk of cyberattack, exploitation, and data breach by malicious parties.

During fiscal year 2023, VITA and the Multisource Service Integrator (MSI) continued to evaluate the current service level measurements to ensure they align with the Commonwealth's needs. VITA and the MSI implemented changes to the service level related to security and vulnerability patching. The changes to this service level included establishing a Common Vulnerabilities and Exposures (CVE) threshold, which required that ITISP suppliers must install any patch with a CVE score above the threshold within 60 days. VITA excluded the revised service level related to security and vulnerability patching from the monthly monitoring process until June 2023 to allow the agency, the MSI, and the ITISP suppliers time to develop procedures and data standardizations to accurately monitor compliance with the service level. VITA should ensure that the CVE score threshold is sufficient to meet the Security Standard requirements and to mitigate the risk associated with the Commonwealth's information, data, and security.

The Security Standard also requires agencies to review and analyze audit records at least every 30 days for indications of inappropriate or unusual activity *(Security Standard, Section AU-6 Audit Review, Analysis, and Reporting)*. Our audits of various agencies for fiscal year 2023 found that agencies rely on 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 2023, 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.

During fiscal year 2023, VITA continued to work with the managed security supplier to address the agencies' inability to access the audit log information. The supplier continued to implement the managed detection and response platform with a small number of agencies piloting the platform in 2023. As of October 2023, the supplier has opened the platform to all Commonwealth agencies. VITA should continue to work with the supplier to ensure all agencies have access to the platform, and all necessary audit logs are available for agency review.

To ensure all agencies that rely on the ITISP services comply with the Security Standard, VITA should ensure suppliers meet all contractual requirements (e.g., key measures, critical service levels, deliverables, etc.). To aid in determining which requirements have Security Standard implications, VITA should crosswalk contractual requirements to the Security Standard. A crosswalk will help in identifying which requirements, if not met, could put an agency at risk, per the Security Standard. If VITA determines suppliers are not meeting any of these requirements, 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.

Improve Oversight of Third-Party IT Service Providers

Type: Internal Control and Compliance

Severity: Significant Deficiency

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 Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment 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 SOC reports for both financial reporting (SOC 1) and IT security (SOC 2). Although VITA obtained and reviewed all required SOC reports for fiscal year 2023, we identified the following weaknesses:

- two of seven (29%) service providers did not provide their 2023 SOC 1 reports to VITA by September 1;

- for four of five (80%) service providers with subservice organizations, VITA did not obtain SOC reports for the subservice organizations or document a justification for why it did not obtain and review the subservice SOC reports;

- for six of six (100%) service providers that include complementary user entity controls in the SOC report, VITA did not document how the agency ensures the controls are in place and operating effectively; and

- for two of two (100%) service providers with qualified opinions, VITA did not properly identify the qualified opinions in the SOC Review Checklists nor document how the qualified opinions potentially affect VITA's operations.

The Hosted Environment Security Standard states that agency heads are accountable for maintaining compliance with the Security Standard, and agencies must enforce the compliance requirements through documented agreements and oversight of service providers. 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, several of the initial checklists were incomplete, including missing documentation for risk ratings, subservice organizations, user control considerations, control objectives, and overall conclusion, which required VITA to revise the checklists. VITA should ensure all staff

responsible for reviewing SOC reports, and completing SOC Review Checklists, receive adequate training on the various components of SOC reports to be able to thoroughly complete the checklists and evaluations.

VITA should work with its service providers to communicate all deadlines and ensure all service providers timely submit SOC reports to VITA to allow time for VITA to complete a thorough review and documentation of the reports. VITA should consider including contract terms with definitive deadlines for SOC report submission so that VITA is able to enforce timely submission of service provider SOC Reports. When VITA identifies modified opinions or exceptions in the SOC reports, VITA should sufficiently document the reasons for the modification of opinion and the assessment of the effect on VITA and the Commonwealth. Additionally, VITA should document the additional actions the agency will take to ensure the service provider sufficiently addresses exceptions.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2023

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

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, 2023. 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 evaluate the accuracy of VITA's financial reporting related to right-to-use assets. In support of these objectives, we 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.

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 contract management, contract payment, centralized information technology security audit service, and right-to-use asset accounting business cycles.

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; observation of VITA's operations; and analytical procedures 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 or noncompliance 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 the Department of 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."

VITA has taken adequate corrective action with respect to 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 a material weaknesses 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, 2023. The Single Audit Report will be available at www.apa.virginia.gov in February 2024.

Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on February 8, 2024. 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

JMR/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective action	First Issued
Conduct Audits of Agency Sensitive Systems Timely	Complete	2022
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

SCHEDULE OF VITA-RELATED RISK ALERTS

The following chart contains agencies included in our audit scope for fiscal year 2023 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 services, which we did not include in our audit scope for fiscal year 2023.

Agency	Report Title	Issued	Risk Alert Title(s)
Department of Accounts	Agencies of the Secretary of Finance for the year ended June 30, 2023	February 2024	Access to Audit Log Monitoring Tool
Department of Behavioral Health and Developmental Services	Agencies of the Secretary of Health and Human Resources for the year ended June 30, 2023	February 2024	Access to Audit Log Monitoring Tool Unpatched Software
Department of Education	Department of Education for the year ended June 30, 2023	February 2024	Access to Audit Log Monitoring Tool Unpatched Software
Department of Health	Agencies of the Secretary of Health and Human Resources for the year ended June 30, 2023	February 2024	Access to Audit Log Monitoring Tool Unpatched Software
Department of Medical Assistance Services	Agencies of the Secretary of Health and Human Resources for the year ended June 30, 2023	February 2024	Access to Audit Log Monitoring Tool Unpatched Software
Department of Motor Vehicles	Agencies of the Secretary of Transportation for the year ended June 30, 2023	February 2024	Unpatched Software
Department of Planning and Budget	Agencies of the Secretary of Finance for the year ended June 30, 2023	February 2024	Access to Audit Log Monitoring Tool
Department of Taxation	Agencies of the Secretary of Finance for the year ended June 30, 2023	February 2024	Unpatched Software

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 8, 2024

BY EMAIL

Ms. Staci Henshaw
The Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218
c/o Mike.Reinholtz@apa.virginia.gov

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, 2023. We commend the time, effort, and professionalism of your staff in completing the assessment and report.

The report identifies three open 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

Right-to-use assets refers to both leased assets, which are the subject of GASB Statement No. 87, and SBITA (subscription-based information technology arrangements) assets, which are the subject of GASB Statement No. 96. As the finding states, these GASB statements have recently become effective and "have dramatically impacted the financial reporting requirements for VITA in the last two years." VITA is unique in the Commonwealth, acting as both a reseller and broker of information technology goods and services on behalf of the public sector entities that we serve. Some of those entities are in the executive branch, and they directly use VITA goods and services. Other public entities are independent agencies, other branches of Government, and localities. For example, we acquire and lease large quantities of computer hardware (such as ~65,000 desktop computers and thousands of servers) and leased software (such as Microsoft and Oracle software licenses) to achieve enterprise volumes and maximize discounts, which we then deliver to the agencies that we serve, who then pay VITA for those goods. Though VITA

acts an intermediary, the end customer agencies are the entities who order and commit to the terms of the leased assets and software subscriptions. Given this complex arrangement, determining the appropriateness and implementation of GASB 87/96 controls required significant interpretation beyond the materials provided by GASB and the Department of Accounts (DOA) CAPP manual.

Applying these GASB statements to the multiple-component (software, hardware, maintenance, labor, etc.) contracts that VITA manages is complex work, particularly given that GASB recognizes a degree of business judgment and discretion in how to apply the statements to such agreements, which has sometimes changed the nature of accounting reporting involved. This activity is further complicated when multiple products are bundled (example, leased server software that is bundled into a leased asset) but delivered as a single product. Notably, VITA recorded Xerox (VITA's Managed Print vendor) and Verizon (VITA's Managed Network vendor) contract assets as fixed last year, but then, after training from a national accounting firm on GASB (per the recommendation from last year's APA audit) and continued communication among VITA, APA, and DOA during the year, APA made a technical inquiry to GASB in November about those contracts, the results of which APA summarized as follows:

> "Today we met with GASB about our technical inquiry. GASB agreed that the Xerox and Verizon contracts are complex agreements that do not easily fit the GASB 87 mold. GASB stated that they could see how you could justify reporting the monthly payments in question as either fixed or variable. They stated it was a judgement call, which they do not provide decisive answers for governments. They did share that if we went with the payments as fixed, there would have to be a reconciliation at year end between what was recorded as a liability versus what was actually paid and an adjustment posted for the difference. Based on GASB's statement that these costs could be reported either way and the administrative burden of reporting them as fixed, we have determined that Xerox and Verizon monthly payments can be reported as variable payments. We met with DOA, and they agreed with this conclusion."

VITA recognizes the extraordinary efforts of the APA audit team in seeking to correctly interpret the GASB guidance and apply it to VITA's complex operating environment. Although VITA understands that agencies are ultimately responsible on their own for interpreting and implementing GASB requirements, VITA has worked to treat assets in a manner consistent with APA and DOA's guidance, and VITA appreciates APA's and DOA's ongoing communications with VITA and assistance in working through the difficult questions that personnel from all involved agencies have had to confront with respect to how to apply the GASB statements in accounting for VITA's contracts.

VITA's IT products and services are unique among Commonwealth agencies, and VITA agrees with APA's assessment that VITA lacks sufficient staffing and financial system resources to perform the extensive and increasingly complex GASB 87/96 compliance and reporting work throughout the year. In recognition of the need for more knowledge and staffing, VITA will seek additional contracted resources while VITA acquires and builds internal talent. VITA will also

seek to improve our financial information and reporting systems to meet the requirements of GASB 87/96. VITA's legacy financial system is over 20 years old and no longer meets the needs of modern financial reporting. VITA will request funding through the budgetary process for improvements to VITA financial management applications.

VITA supports and agrees with APA's direction to provide more financial reporting clarity on the descriptions and categorizations of expenses and assets that are delivered to the Commonwealth's agencies. Though this material weakness finding does not impact VITA's income, expenses, or budget; the IT service rates paid by VITA's customer agencies will not change; and supplier payment amounts under the relevant contracts do not increase; VITA remains committed to maintaining and enhancing the integrity of our financial reporting.

Finding title: Continue to Ensure ITISP Suppliers Meet all Contractual Requirements

Ensuring that infrastructure suppliers fulfill all contractual requirements with respect to Commonwealth security policies and standards necessitates a programmatic, continuous improvement approach. VITA has made improved cybersecurity a primary goal and major initiatives have completed and are underway. Improvements in 2024 include the tokenization of privileged administrator accounts, requirement of more complex passwords, installation of improved cybersecurity software (Nucleus, Nessus, Splunk, CyberArk, Accunetix), deployment of statewide cybersecurity awareness training, vaulting of critical data, and start of improved identity management. Improving vulnerability remediation (including patching) and providing agencies with direct access to their incident logs has been a focus over the past two fiscal years, and those efforts have come to fruition in 2023, albeit after the June 30 end of the audit period.

To continuously address vulnerabilities, VITA has established a scoring mechanism, based on the Common Vulnerability Scoring System (CVSS), that delineates the necessary response based on the criticality of the vulnerability (critical, high, and medium). For vulnerabilities with a CVSS score of 7.0 and higher (critical and high), service level agreement (SLA) 1.1.3 is now in place to measure supplier performance and adjust supplier compensation accordingly through SLA credits and RCDs. For vulnerabilities below 7.0, in Q4 of 2023, suppliers started providing data in a quarterly report to the MSI and VITA. The new SLAs combined with the reports of vulnerabilities below 7.0 are used to ensure suppliers' contractual compliance.

VITA's data shows that patches for software on the enterprise software list are being applied, both on an ongoing basis and in reduction of past backlog. Indeed, according to our Security Center console, 122,998 vulnerabilities were remediated in the last 30 days. VITA will work with agencies and suppliers if there are any new technical difficulties or questions about patching.

New tools are also making a difference. Splunk and Nucleus are now available to agencies so that they can monitor and verify the remediation of the vulnerabilities for which infrastructure suppliers are responsible. The Splunk and Nucleus dashboards have also been provided to the

suppliers so that they can review a shared and common vulnerability list. Prior to this action, the suppliers and the Commonwealth sometimes had differing views regarding the vulnerabilities in the environment.

VITA and the suppliers monitor and review enterprise level logs and security events on behalf of customer agencies through the enterprise managed detect and response (MDR) system and a 24x7 Security Operations Center. The MDR dashboard is available for access by agencies as of Q4 2023. The agencies have real-time, drill-down insight into enterprise security alerts and events in their environment. The MDR dashboard also contains a "Security Data Lake" tab which allows agencies to run queries on all agency related logs collected by the tool. Agency access is based on agency submission of a request.

A recent security audit by the IRS has provided evidence of current security success. The Commonwealth and the infrastructure services suppliers successfully completed a security audit by the IRS where all software, devices, and infrastructure processing FTI (Federal Tax Information) data were scanned. The suppliers were held accountable to remediate the IRS security team's findings, and the Commonwealth successfully passed the audit.

The effectiveness of the infrastructure services security and program improvements can be evidenced by these positive outcomes in 2023. VITA will continue to monitor and improve the security of infrastructure services through ongoing governance, including the requirements of architecture documentation, system security plans, and audit reports. VITA's infrastructure services group will work with our security group to confirm that the current state achieves security standards compliance. VITA looks forward to demonstrating our improvements and compliance in the FY24 APA audit.

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

This finding pertains to VITA's oversight of IT infrastructure suppliers, a key group of businesses who are part of VITA's multi-sourcing services integrator (MSI) model for the provision of IT infrastructure services to executive branch agencies. The MSI model involves extensive contracts and relationships between VITA and a core group of infrastructure suppliers who each provide a set of services (referred to as a services "tower"), along with one supplier (SAIC) who is the MSI – the integrator, coordinator, and provider of certain cross-functional services. The contracts provide a variety of governance processes and potential enforcement mechanisms and remedies.

VITA's contracts with IT infrastructure suppliers require those providers to submit SOC2 reports annually. Those SOC report submissions are deliverables tracked under the contract, and if a supplier is late in submitting a SOC report, VITA follows up and, if need be, opens a governance case to press for resolution. This year, for example, although the audit correctly notes that two suppliers did not provide SOC reports by September 1, VITA did receive those SOC reports within a month thereafter and reviewed them.

IT infrastructure suppliers may use subcontractors or work together with other companies to provide a tower of services. For example, VITA's Messaging Services are provided by NTT Data, using a Microsoft 365 platform for which VITA also contracts directly with Microsoft. Through those contracts and cloud oversight processes, VITA will independently obtain and review SOC reports from entities like Microsoft with whom VITA contracts directly for software or other service components. But VITA does not exercise that type of direct oversight with respect to every subcontractor an infrastructure services tower supplier may use; instead, under the MSI model contracts, each supplier is contractually responsible for its subcontractors and for providing its services in compliance with Commonwealth security policies and standards. VITA then exercises oversight and governance over the tower suppliers, aided by the MSI.

In general, the security oversight of IT infrastructure services suppliers is working and effective. VITA agrees with the finding, however, that there is a need to mature and improve process and review documentation. VITA plans to investigate whether an earlier delivery or more review time is needed to obtain and review the SOC documentation. VITA appreciates APA's review of this important oversight process and the specific guidance as to where APA believes improved documentation is needed.

Thank you again for your staff's work, insight, and commitment to our success.

Sincerely,

Robert Osmond

Robert Osmond

cc (by email): Secretary of Administration Lyn McDermid