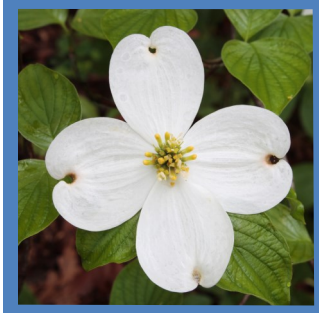

VIRGINIA INFORMATION TECHNOLOGIES AGENCY

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2022

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

AUDIT SUMMARY

We have audited the Virginia Information Technologies Agency's (VITA) contract management, centralized information technology security audit service, and leased asset accounting business cycles for the fiscal year ended June 30, 2022. We found:

- proper recording and reporting of leases, 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 Leased 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; and

- one instance 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' management that requires the action and cooperation of VITA. Our separate audit report for each agency includes the details of each risk that we identified.

-TABLE OF CONTENTS-

	Pages
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-4
INDEPENDENT AUDITOR'S REPORT	5-7
APPENDIX A – SCHEDULE OF VITA-RELATED RISK ALERTS	8
AGENCY RESPONSE	9-14
AGENCY OFFICIALS	15

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Improve Controls over Identifying, Tracking, Recording, and Reporting Leased Assets
Type: Internal Control
Severity: Material Weakness
Repeat: No

Virginia Information Technologies Agency's (VITA) management and Finance Department did not plan and prepare for the implementation of Governmental Accounting Standards Board (GASB) Statement No. 87 to ensure proper identification and reporting of leases. GASB delayed the GASB Statement No. 87 implementation by one year, which provided state agencies additional time to prepare for this new accounting standard over leased assets. However, VITA's implementation process was still deficient in the following areas, resulting in misstatements ranging from $539,000 to $111.1 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. We noted the following deficiencies in VITA's process:

- The Finance Department did not review contract documents or work with other departments within VITA to identify the complete population of leases. As a result, they excluded the largest contract involving lease assets, understating right to use assets and the associated long-term lease liability by $96.7 million.

- The Finance Department did not consistently determine the lease term and asset grouping of the leases across all contracts.

- The Finance Department misinterpreted the Department of Account's (Accounts) policies and procedures by using the prime rate for a group of assets within one contract instead of determining VITA's incremental borrowing rate for the assets as GASB Statement No. 87 requires.

- The Finance Department did not document and retain its reconciliation process for verifying and ensuring the completeness and accuracy of the leased asset data the vendor provided for use in valuing VITA's lease assets and liabilities.

- The Finance Department did not develop GASB Statement No. 87 implementation policies and procedures to ensure consistent application across contracts.

VITA provides this information to Accounts for its internal service funds through a financial statement template for inclusion in the Commonwealth's Annual Comprehensive Financial Report (ACFR). We consider the combination of issues noted to be a material weakness 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 Statement No. 87 prescribes the applicable accounting standards surrounding the proper accounting and financial reporting for leases. Commonwealth Accounting Policies and Procedures (CAPP) Manual Topics 31205 through 31220 state all agencies must follow guidelines as required by GASB Statement No. 87, and the Commonwealth's lease accounting system users should review the specific requirements of the statement. CAPP Manual Topic 31205 specifically states that the lessee should determine the discounted interest rate using the implicit or explicit rate in the contract or the lessee's estimated incremental borrowing rate prior to using the Commonwealth's default prime rate.

VITA's Finance Department did not have an accurate understanding of GASB Statement No. 87 and did not attend the necessary training to be able to properly plan, prepare, and implement GASB Statement No. 87. VITA's management should ensure the individuals evaluating, tracking, recording, and reporting leases obtain training and the appropriate resources to ensure they have a thorough understanding of the requirements of GASB Statement No. 87. Management should develop, implement, and update policies and procedures regularly over their leased-asset process to ensure accurate and complete reporting. In addition, they should perform an evaluation over all VITA contracts to ensure the Finance Department properly captures all leases, corrects any misstated leases, and enters all lease data in the Commonwealth's lease accounting system. Furthermore, VITA should retain records of all implemented controls 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
Repeat: Yes (first issued in fiscal year 2020)
Prior Title: Ensure ITISP Suppliers Meet all Contractual Requirements

Although VITA is monitoring and enforcing the contractual requirements each month, as of June 2022, 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), 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 the 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 2022 found critical and highly important security patches that were past the 90-day Security Standard requirement.

The systems missing critical security updates are at an increased risk of successful cyberattack, exploit, and data breach by malicious parties.

Additionally, the Security Standard 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 2022 found that agencies rely on the ITISP suppliers to provide access to a centralized monitoring tool that collects audit log information about activities in the information technology (IT) environment. Certain agencies were unable to obtain access to the audit log information during fiscal year 2022, and thus were not able to comply with the Security Standard requirements related to audit log monitoring. Although the supplier was performing audit logging and monitoring, only a select few agencies have access to the monitoring tool while the supplier is pilot testing the tool. The Commonwealth's risk associated with data confidentiality, integrity and availability increases with agencies not being able to review and monitor their individual audit logs.

During fiscal year 2022, VITA and the Multisource Service Integrator (MSI) evaluated the current service level measurements to ensure they align with the Commonwealth's needs. As of December 2022, VITA and the MSI are implementing changes to the service level related to security and vulnerability patching. The changes to this service level include establishing a Common Vulnerabilities and Exposures (CVE) threshold. The new security and vulnerability patching service level will require the ITISP suppliers to install any patch with a CVE score above the threshold within 90 days.

VITA continues to work with the managed security supplier to address the agencies' inability to access the audit log information. The supplier replaced the original security incident and event management system with a new managed detection and response (MDR) platform. Currently, only a small number of agencies are piloting the new MDR system.

VITA should document the rationale for all changes to the service levels, including the basis for the CVE score threshold selected, and continually reevaluate the service levels as risks change. To ensure all agencies that rely on the ITISP services can comply with the Security Standard, VITA should ensure ITISP suppliers meet all contractual requirements (e.g., key measures, critical service levels, deliverables). 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 an ITISP supplier is not meeting a contractual requirement that may have a Security Standard implication, VITA should communicate with the affected agencies and provide guidance on compensating controls and processes the agencies should implement to reduce risk while the suppliers work to meet the requirements of the contract.

Conduct Audits of Agency Sensitive Systems Timely
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

VITA's Centralized IT Security Audit Service (Audit Services) conducts IT security audits for contracted agencies. The Commonwealth's Information Technology Security Audit Standard, SEC 502 (Security Audit Standard), Section 2.1, requires agencies to complete security audits for each sensitive system every three years from the last audit completion date. Based on our review of audit completion dates provided by Audit Services, we determined the following:

- During fiscal year 2022, Audit Services completed four of six agency IT security audits after the three-year audit deadline.

- As of June 30, 2022, Audit Services is currently engaged, or has not started, ten agency IT security audits that are past the three-year audit requirement.

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 audit. Audit Services audits all the systems in scope for an agency at the same time and issues one audit report covering all systems in scope per the MOU. Audit Services should consider adding information to the MOU related to audit deadlines or planned timeframe for the audit. This added communication will ensure all parties understand when Audit Services plans to complete the audits. Additionally, more information regarding audit timing will allow agencies to determine if they need to obtain a separate audit for specific systems to ensure those systems remain compliant with the Security Audit Standard between the date of the MOU and the anticipated deadline set by Audit Services.

Of the four audits Audit Services completed late during fiscal year 2022, two of the delays are due to the agencies requesting postponements. Additionally, of the ten audits that were already late as of June 30, 2022, two are due to agency-requested postponements. The remaining late audits are primarily due to resource constraints within Audit Services. Audit Services should regularly monitor its audit workplan to ensure audit staff complete all IT security audits by the required deadlines. Additionally, Audit Services should evaluate its staffing levels and assess if VITA should contract with an outside audit 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, 2022

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

We have audited the contract management, centralized information technology security audit service, and leased asset accounting business cycles of the **Virginia Information Technologies Agency (VITA)** for the year ended June 30, 2022. 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 the contract management and centralized information technology audit service and evaluate the accuracy of VITA's financial reporting related to leases. In support of these objectives, we tested for compliance with applicable laws, regulations, and contract agreements and reviewed corrective actions with respect to an audit finding and recommendation from the prior year report. Additionally, we evaluated the accuracy of reported leases in the Commonwealth's lease accounting system and Department of Accounts' financial statement template.

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, centralized information technology audit service, and leased 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, and contract agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of VITA's operations to achieve our 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 Leased 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 "Conduct Audits of Agency Sensitive Systems Timely," 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 Department of Accounts' financial statement

template, after adjustment for the misstatements noted in the finding "Improve Controls over Identifying, Tracking, Recording, and Reporting Leased Assets."

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, and contract 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 not taken adequate corrective action with respect to the previously reported finding titled "Ensure ITISP Suppliers Meet all Contractual Requirements." Accordingly, we included this finding 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 deficiency, 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, 2022. The Single Audit Report will be available at www.apa.virginia.gov in February 2023.

Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on January 30, 2023. 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 it.

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/vks

APPENDIX A

Schedule of VITA-Related Risk Alerts

The following chart includes agencies included in our audit scope for fiscal year 2022 and impacted by the findings titled "Continue to Ensure ITISP Suppliers Meet all Contractual Requirements" and "Conduct Audits of Agency Sensitive Systems Timely." These findings also impact other agencies that rely on VITA services, which we did not include in our audit scope for fiscal year 2022.

Agency	Report Title	Issued	Risk Alert Title(s)
Department of Accounts	Agencies of the Secretary of Finance for the year ended June 30, 2022	February 2023	Access to Audit Log Monitoring Tool Timely Security Audits
Department of Behavioral Health and Developmental Services	Agencies of the Secretary of Health and Human Resources for the year ended June 30, 2022	February 2023	Access to Audit Log Monitoring Tool Unpatched Software
Department of Education	Department of Education for the year ended June 30, 2022	January 2023	Access to Audit Log Monitoring Tool Unpatched Software Timely Security Audits
Department of Health	Agencies of the Secretary of Health and Human Resources for the year ended June 30, 2022	February 2023	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, 2022	February 2023	Access to Audit Log Monitoring Tool Unpatched Software
Department of Motor Vehicles	Agencies of the Secretary of Transportation for the year ended June 30, 2022	February 2023	Unpatched Software
Department of Taxation	Agencies of the Secretary of Finance for the year ended June 30, 2022	February 2023	Unpatched Software

COMMONWEALTH of VIRGINIA

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

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

TDD VOICE -TEL. NO.
711

February 6, 2023

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) welcomes the opportunity to respond to the combined audit of VITA's contract management, centralized information technology security audit service, and leased asset accounting business cycles covering the fiscal year that ended on June 30, 2022. Thank you to your staff for their time and diligence in drafting the assessment and recommendations.

There were three items noted on this audit related to internal controls, including one repeat finding. Each of these items is addressed separately below.

Improve Controls over Identifying, Tracking, Recording, and Reporting Leased Assets
Type: Internal Control
Severity: Material Weakness
Repeat: No

Prior to responding to the leased asset finding in the report, it is important to begin by noting the situation that agencies (including the Auditor of Public Accounts) have faced with respect to Governmental Accounting Standards Board (GASB) Statement No. 87. GASB 87 is a 96-page, complex, new accounting policy that is still evolving, going through the process for clarifying and defining the requirements for agency compliance. At the time of this audit, the GASB 87 requirements were in the first year of being newly implemented. Although official training was provided on the audit system, there was little to no Commonwealth training available on interpretation and implementation of the GASB 87 requirements. There were no guidelines, definitions, or examples available from Commonwealth of Virginia official sources to enable assessment of which contracts fall under the purview of the GASB 87 standards. For example, a checklist to determine whether a leased asset is subject to GASB 87 does not exist. As of today, no GASB 87 training is listed as available on the Department of Accounts (DOA) website or any other Commonwealth source. General training on lease accounting is available, and VITA

participated in that training. However, given the newness of the standard's implementation, agencies still had to interpret the complex GASB 87 requirements with respect to leased assets and then develop and align their internal controls and reporting activities based on that definition.

VITA's management and Finance Department planned and prepared for the implementation of GASB 87 to ensure proper identification and reporting of leases. VITA staff researched and took pertinent training that was available through a private entity. The agency's Assistant Controller and other agency staff met with staff from DOA and APA over a four-month period from February 2022 through May 2022, initially monthly and then weekly to discuss and address compliance concerns, develop a plan, review the plan, and come to a mutually agreeable solution for implementation of GASB 87. VITA's understanding of which contracts were subject to GASB 87 was informed by those discussions and meetings. VITA is grateful for the support provided by the DOA and APA through this period.

Despite this coordination and further inquiries to APA requesting clarification and guidance (including in the course of this audit), the definition of what constitutes a leased asset remains unclear to VITA. VITA's understanding based on the responses to our inquiries is that the definition of a leased asset, as of the time of this report, is subjective and necessitates decomposing IT services contracts into lease and non-lease components and weighing many factors. Interpretation and judgment are required, and given the newness of the GASB 87 implementation, insufficient precedents and examples existed that could be used to inform VITA's Finance Department.

During the APA's audit of VITA leased assets, APA determined that VITA's implementation process was insufficient and had resulted in misstatements ranging from $539,000 to $111.1 million for various financial statement line items, including the intangible right to use capital assets, long-term liabilities, amortization, rent, and interest expense, as well as the associated footnote disclosures. This determination was based on APA's inclusion of an on-demand voice and data network services contract to be within the scope of contracts under the purview of GASB 87.

- VITA's Finance Department comprehensively reviewed contract documents and worked with other departments within the agency to identify the population of leases subject to GASB 87. VITA remains unsure that the financial statements for the on-demand voice, data, and network services contract should have been subject to GASB 87 because that contract does not include lease obligations. There are no lease terms for the services in that contract. That contract is structured as purely a consumption contract (for example, ordering phone or broadband service). Consumers and VITA can vary consumption of services at-will each month, and consumption could go to $0 if consumers elect to disconnect contract services, without any penalties. VITA deferred to the APA's interpretation of GASB 87 and is now applying APA's interpretation, restating VITA's financials to include the on-demand voice, data, and network services contract in accordance with APA's interpretation.

- Based on APA's interpretation of a leased asset, our Finance Department agrees that we did not consistently apply the lease term (which APA identified as the life of the contract based on historic use) and asset grouping of leases across all contracts.

- VITA's Finance Department agrees with the APA that VITA misinterpreted DOA's policies and procedures by using the prime rate for a group of assets within one contract instead of determining our incremental borrowing rate for the assets as required by GASB 87.

- VITA's Finance Department did not sufficiently develop GASB 87 implementation policies and procedures to ensure consistent application across contracts. As our understanding of GASB 87 matures, we are currently in the process of updating written procedures to support adequate processes going forward.

Based on APA's interpretation of GASB 87, we anticipate that future reclassifications may be warranted. During the exit interview, VITA learned that the APA was applying a standard of historic use. If such a standard is applied, then further analysis may be required to determine whether additional contracts may also be subject to GASB 87. For example, VITA offers other telecommunications contracts to state agencies and localities for mobile and telephone services, including mobile phones, MiFi hotspots, air routers, conference equipment, and desk phones. Like the on-demand voice, data, and network contract mentioned earlier, none of the items on these contracts include lease obligations, but if the standard of historic use is applied, then additional analysis, interpretation, and judgment may be necessary.

VITA's Finance Department will consult with outside subject matter experts to determine the extent to which any future modifications are warranted. We have secured an industry-leading external consultant to guide the process of documenting the reconciliation process and will retain sufficient evidence to verify and ensure the completeness and accuracy of the leased asset data provided by the vendor for use in valuing VITA's leased assets and liabilities going forward. We anticipate that the work products produced may benefit the Commonwealth as a whole, and we will freely share such materials with the APA, DOA, and any other agency.

VITA will also be securing additional training for all VITA Finance Department staff to be able to improve implementation of GASB 87. VITA's management will ensure the individuals evaluating, tracking, recording, and reporting leases obtain training and the appropriate resources to ensure they have as thorough and clear an understanding of the requirements of GASB Statement No. 87 as possible going forward. Management will also develop, implement, and update policies and procedures regularly over our leased asset process to ensure accurate and complete reporting. In addition, we will perform an evaluation over all VITA contracts to ensure the Finance Department has properly captured all leases, corrected any misstated leases, and entered all lease data in the Commonwealth's lease accounting system. Furthermore, VITA will retain records of all implemented controls such as reconciliations to mitigate the risk of vendor information being inaccurate in comparison to the contract and payments made to vendors.

Finally, we note that the finding on GASB 87 reporting does not impact VITA's income or expenses. In other words, VITA's budget is not affected by this audit; the IT service rates paid by VITA's customer agencies will not change because of this audit; and supplier payment amounts under the relevant contracts do not increase as a result of this audit.

VITA appreciates that properly recognizing and identifying appropriate leased assets improves financial transparency and promotes better fiduciary governance. We have worked collaboratively and transparently with APA to address this issue, and we look forward to the help of the expert consultants to ensure that VITA improves our future compliance.

Continue to Ensure ITISP Suppliers Meet all Contractual Requirements
Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2020)
Prior Title: Ensure ITISP Suppliers Meet all Contractual Requirements

VITA agrees that cybersecurity is a critical priority. As APA notes in this year's audit, VITA is continuing to monitor and improve services within the Commonwealth's enterprise IT environment. VITA has established processes to assess the security of enterprise IT services, and VITA continues to make progress with respect to the issues discussed in this finding.

Remediating vulnerabilities, which includes patching, is a complex challenge and process in a sizable enterprise. The enterprise will never be vulnerability-free, with hundreds of thousands of devices and patches being released continually, but recent progress is notable by any measure. VITA, working with our multi-sourcing services integrator (MSI), opened a multi-supplier project to reduce and eliminate unremediated vulnerabilities. The results of that project are as follows:

- 95% of critical enterprise vulnerabilities were addressed and eliminated;
- 100% of Servers are now reporting to the vulnerability management system properly;
- the Server Supplier is trending towards a 100% remediation of vulnerability patches older than 90 days old by the end of August 2023;
- 95% of workstations are linked to the vulnerability management system;
- the End-User Services (including workstations) provider is trending towards a 100% remediation of vulnerability patches older than 90 days old by the end of September 2023;
- the Managed Security Services Supplier is currently scanning 96% of devices they provide and is on track to be scanning all devices by the end of August 2023; and,
- the Managed Security Services Supplier is trending towards a 100% remediation of vulnerability patches older than 90 days old by the end of September 2023.

VITA also is beginning to apply a meaningful vulnerability remediation service level that prioritizes significant vulnerabilities and is based on industry standards. Effective with the monthly performance period beginning April 1, 2023 (due to contractual notice periods before service level changes take effect), SLA 2.3.4 will measure the IT infrastructure suppliers against a requirement that 97% of vulnerabilities with a CVSS of 7.0 or higher are remediated within 60 days. "CVSS" stands for Common Vulnerability Scoring System, a vulnerability severity level assessment system associated with the Common Vulnerabilities and Exposures (CVE) standard, which is sponsored by the Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA). A score of 7.0 is the bottom of the "high" priority range. This approach to prioritizing vulnerability remediation is part of VITA's larger alignment of Commonwealth security standards with federal standards and industry best practices.

Holding suppliers accountable is more than simply sitting back and assessing service level credits – vulnerabilities at all severity levels will be noted in scans and addressed. But this revision of SLA 2.3.4 ensures that service level credits (available beginning with June performance) are focused on quick remediation of the most significant vulnerabilities.

With respect to agency access to security log information, all logs are being monitored. 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. Agencies have direct access to agency-relevant security posture information via a security dashboard. VITA believes this approach is sensible and will continue to build out this approach to compliance with Commonwealth security standards.

VITA intends to further enhance services during the remainder of calendar year 2023 by (1) establishing an additional MDR dashboard to give agencies current, drill-down insight into enterprise security alerts and events that are occurring within their environment; and (2) sending enterprise logs to cloud containers that allow agencies to perform reviews and queries in a manner of their choosing. VITA is also working on additional tools and implementation of zero trust, which will further enhance security and compliance.

The security compliance of enterprise IT services overall is assessed on an ongoing basis through System Security Plan (SSP) submission and review, an established process applicable to all of the IT infrastructure suppliers.

We welcome the opportunity to continue showing our progress improving IT infrastructure security and closing out this finding. To that end, we invite you and your staff to continue working with VITA to see what we are doing to ensure IT infrastructure services are secure and compliant with standards and thereby promote faster resolution.

Conduct Audits of Agency Sensitive Systems Timely
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

VITA appreciates the recommendation to consider adding information to the MOU about the audit deadlines or planned timeframes for audit completion. VITA agrees that deadlines or planned timeframes need to be memorialized. Audit workplans that are created with the agencies are the most appropriate place to memorialize this information. Once the agencies sign the MOU, they submit an audit workplan to VITA, and the audit workplan determines the timeframes for Audit Services to audit the agency's systems and sets forth an agreed auditing schedule. The cycle to audit agency systems every three years commences when the agencies sign the MOU and submit the audit workplan. The current MOU and audit workplan approach allows customer agencies to decide whether they want to audit certain systems separately from the auditing conducted through Audit Services to ensure compliance with the Security Audit Standard.

With respect to the timeliness of IT security audits, VITA agrees that timely audits are important. Audit Services will regularly monitor the audit workplans and evaluate staffing levels to complete audits by the required deadline.

VITA will continue to work diligently to improve cybersecurity across the Commonwealth, including through security in our IT infrastructure services. Thank you again for your staff's work on this review, and we look forward to working with you in the future.

Sincerely,

Robert Osmond

cc (by email): Secretary of Administration Lyn McDermid

VIRGINIA INFORMATION TECHNOLOGIES AGENCY

As of June 30, 2022

Robert Osmond
Chief Information Officer

Michael Watson
Chief Information Security Officer

Cynthia Cordova-Edwards
Chief Financial Officer

Dan Wolf
Chief Administrative Officer