



VIRGINIA INFORMATION TECHNOLOGIES AGENCY

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2021

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 business cycle for the period of July 1, 2020, through June 30, 2021. We found:

- one matter involving internal control and its operation necessary to bring to management's attention; and
- no 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' management that requires the action and cooperation of VITA. Our separate audit report for each agency includes the details of each risk we identified.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS	1-2
INDEPENDENT AUDITOR'S REPORT	3-5
APPENDIX A: SCHEDULE OF VITA-RELATED RISK ALERTS	6
AGENCY RESPONSE	7-8
AGENCY OFFICIALS	9

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Ensure ITISP Suppliers Meet all Contractual Requirements

Type: Internal Control

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2020)

The Virginia Information Technologies Agency (VITA) is responsible for the operation, governance, and security of the Commonwealth's technology infrastructure. From 2005 to 2018 the Commonwealth, with oversight and governance by VITA, contracted with a single provider for information technology (IT) infrastructure services. In 2018, VITA terminated the contract with the single provider and moved to a multisource environment with seven separate suppliers and one multisource service integrator providing the IT infrastructure services. Agencies of the Commonwealth rely on the services provided by the suppliers through the Information Technology Infrastructure Services Program (ITISP).

Although VITA is monitoring and enforcing the contractual requirements each month, as of June 2021 there were still cases of ITISP suppliers not meeting the minimum requirements. When ITISP suppliers do not meet all contractual requirements (key measures, critical service levels, deliverables, etc.), this 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). Appendix A contains a list of the agencies where we have included a risk alert in their separately issued audit report related to their inability to comply with the Security Standard due to ITISP suppliers not meeting minimum contractual requirements.

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 2021 found a significant number of critical and highly important security patches that were past the 90-day Security Standard requirement (See Appendix A). The systems missing critical security updates are at an increased risk of 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 2021 found that agencies rely on an ITISP supplier to provide access to a centralized monitoring tool that collects audit log information about activities in the IT environment. The agencies were unable to obtain access to the audit log information during fiscal year 2021, and thus were not able to comply with the Security Standard requirements related to audit log monitoring (See Appendix A). Although the supplier was performing audit logging and monitoring, there were challenges with granting agencies access to their

data in the monitoring 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 the initial periods of transition to a multi-supplier environment (beginning in December 2018), the new suppliers under the ITISP were not able to report their status related to the critical service levels, key measurements, or critical deliverables. For example, VITA did not require the ITISP suppliers to report the status of a service level agreement (SLA) related to security and vulnerability patching until October 2019. Through the efforts of VITA and the Multisource Service Integrator (MSI), as of June 2021, all ITISP suppliers provide data or reports to the MSI for each monthly service-level requirement.

VITA and the MSI have been working to evaluate the current service-level measurements. This will allow VITA and the MSI to improve the service-level measurements and better align with the Commonwealth's needs. As of December 2021, the service levels related to security and vulnerability patching are currently undergoing this review and evaluation. Additionally, to help address the risks associated with patching, VITA has worked with the various suppliers to develop an Enterprise Security Software Patching List, a master listing of applications and systems supported by the ITISP suppliers. If an agency identifies uninstalled security and vulnerability patches, the agency will first need to determine if an ITISP supplier supports the related application. If the ITISP suppliers do not support the application, it is the individual agency's responsibility to install the required patches. VITA and the ITISP suppliers finalized the Enterprise Security Software Patching List in August 2021. Between December 2018 and August 2021 there was no master list for agencies to check for validation.

VITA continues to work with the ITISP suppliers to address the agencies' inability to access the audit log information. The responsible supplier is replacing the original security incident and event management (SIEM) system with a new managed detection and response (MDR) platform. While the supplier deploys MDR agents on all servers, the original SIEM platform remains operational. Beginning in January 2022, the supplier will begin discontinuing the SIEM platform. VITA plans for the MDR platform to be fully operational by March 2022, which will enable all agencies to access their respective audit logs for review.

To ensure all agencies that rely on the ITISP services comply with the Security Standard, VITA should ensure ITISP suppliers meet all contractual requirements (key measures, critical service levels, and deliverables). To aid in determining which requirements have Security Standard implications, VITA should crosswalk contractual requirements to the Security Standard. This 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 what the agencies can do to comply with the Security Standard while the suppliers work to meet the requirements of the contract.



Staci A. Henshaw, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2021

The Honorable Glenn Youngkin
Governor of Virginia

The Honorable Kenneth R. Plum
Chairman, Joint Legislative Audit
and Review Commission

We have audited the contract management business cycle of the **Virginia Information Technologies Agency (VITA)** for the period July 1, 2020, through June 30, 2021. 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 objective was to evaluate the adequacy of VITA's internal controls over the contract management business cycle. In support of this objective, 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.

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 business cycle.

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, observation of VITA's operations, and analytical procedures 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. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify a deficiency in internal control titled "Ensure ITISP Suppliers Meet all Contractual Requirements" which is described in the section titled "Internal Control Findings and Recommendations," that we consider to be a significant deficiency.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Conclusions

We noted a matter involving internal control and its operation that requires management's attention and corrective action. This matter is described in the section titled "Internal Control Findings and Recommendations." The results of our tests of compliance with applicable laws, regulations, and contract agreements disclosed no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

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 Findings and Recommendations.”

Since the finding noted above has been identified as a significant deficiency, it 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, 2021. The Single Audit Report will be available at www.apa.virginia.gov in February 2022.

Exit Conference and Report Distribution

We discussed this report with management on January 27, 2022. Management’s response to the finding and recommendation identified in our audit is included in the section titled “Agency Response.” We did not audit management’s response 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

Agency	Report Title	Issued	Risk Alert Title(s)
Department of Accounts	Agencies of the Secretary of Finance for the year ended June 30, 2021	Planned issuance February 2022	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, 2021	Planned issuance February 2022	Access to Audit Log Monitoring Tool Unpatched Software
Department of Education	Department of Education for the year ended June 30, 2021	January 2022	Access to Audit Log Monitoring Tool Unpatched Software
Department of General Services	Department of General Services for the Year Ended June 30, 2020	December 2021	Improve Audit Log Monitoring
Department of Health	Agencies of the Secretary of Health and Human Resources for the year ended June 30, 2021	Planned issuance February 2022	Unpatched Software
Department of Medical Assistance Services	Agencies of the Secretary of Health and Human Resources for the year ended June 30, 2021	Planned issuance February 2022	Access to Audit Log Monitoring Tool Unpatched Software
Department of Motor Vehicles	Agencies of the Secretary of Transportation for the year ended June 30, 2021	Planned issuance February 2022	Unpatched Software
Department of Taxation	Agencies of the Secretary of Finance for the year ended June 30, 2021	Planned issuance February 2022	Unpatched Software



COMMONWEALTH of VIRGINIA

Phil Wittmer
Chief Information Officer
Email: cio@vita.virginia.gov

Virginia Information Technologies Agency

11751 Meadowville Lane
Chester, Virginia 23836-6315
(804) 416-6100

TDD VOICE -TEL. NO.
711

January 28, 2022

BY EMAIL

Ms. Staci Henshaw
The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 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 procurement, management, and billing cycles, covering April 1, 2020, through June 30, 2021. We welcome assessment and recommendations from outside VITA and thank your staff for their time and effort on this audit report.

The only finding from this audit period is a continuation of the finding from last year: "Ensure ITISP Suppliers Meet all Contractual Requirements," highlighting specifically requirements related to compliance with Commonwealth security standards. As VITA wrote last year, we agree with the importance of ensuring that infrastructure suppliers provide services in compliance with Commonwealth security standards.

Last year's VITA response letter described the history of the executive branch information technology (IT) infrastructure platform and the significant progress made on all fronts through modernization and the implementation of the multisupplier model.

As the report from this audit period itself describes, progress has continued toward resolving the finding, including through publication of enterprise software lists that clarify patching responsibilities and through replacement of the original security incident and event management (SIEM) system with a modernized and more capable managed detection and response (MDR) platform.

This work is close to completion and is expected to finish this quarter. Agency information security officers (ISOs) have already been given a preview of the dashboards that the new MDR platform will provide and have responded positively. Rollout of the dashboards to pilot agencies

AN EQUAL OPPORTUNITY EMPLOYER

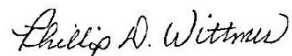
is expected in the first week of February, with the target of reaching the rest of the agencies before the end of this quarter.

VITA's patching information shows that suppliers are currently patching systems in compliance with their service level agreements (SLAs), and the backlog reflecting past patching difficulties continues to shrink and has been reduced by more than half. VITA is continuing to drive improvement in this area.

The enterprise IT infrastructure services platform uses advanced security technology and services based on both Commonwealth security standards and key industry principles, such as defense-in-depth. As you are aware, the infrastructure services contracts are structured to require that the services provided are in compliance with Commonwealth security standards. To ensure that those requirements are met, and in furtherance of resolving this finding, platform security personnel are performing an assessment that includes crosswalking platform security to the security standard to ensure that the contractual requirements are met.

VITA will continue to work diligently to ensure security in our IT infrastructure services and to finish the pending work that will close out the finding in this audit. Thank you again for the review, and we look forward to working with you in the future.

Sincerely,



Phil Wittmer

cc (by email): Noah Johnson, APA

VIRGINIA INFORMATION TECHNOLOGIES AGENCY

As of June 30, 2021

Nelson P. Moe
Chief Information Officer

Michael Watson
Chief Information Security Officer

Jonathan Ozovek
Chief Operating Officer

Dan Wolf
Chief Administrative Officer