VIRGINIA IT AGENCY

REPORT ON AUDIT
FOR THE PERIOD
JULY 1, 2017 THROUGH MARCH 31, 2020

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

AUDIT SUMMARY

We have audited the **Virginia IT Agency's (VITA**) contract procurement business cycle for the period of July 1, 2017, through December 31, 2018. In addition, we audited VITA's contract management and billing cycles for the period of January 1, 2019, through March 31, 2020. 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.

-TABLE OF CONTENTS-

AUDIT FINDINGS AND RECOMMENDATIONS

Ensure ITISP Suppliers Meet all Contractual Requirements
Type: Internal Control
Repeat: No

The Virginia IT 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 the contractual requirements each month, as of March 2020, there were still cases of ITISP suppliers not properly reporting the data or not meeting the minimum requirements. If the ITISP suppliers do not meet all contractual requirements, Commonwealth agencies that rely on the ITISP services may not be in compliance 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 the Department of Taxation and the Department of Education (Education) for fiscal year 2020 found a significant number of 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 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 audit of Education for fiscal year 2020 found that Education relies on the ITISP suppliers to provide Education access to a centralized monitoring tool that collects audit log information about activities in Education's IT environment. Education was unable to access the monitoring tool and audit log information during fiscal year 2020 and thus, was not able to comply with the Security Standard requirements related to audit log monitoring. Although the supplier was performing audit logging and monitoring, there were challenges with granting agencies access to their data in the monitoring tool. Without the agencies being able to review and monitor their individual audit logs, the risk associated with the Commonwealth's data confidentiality, integrity, and availability is increased.

During the initial periods of transition from the single supplier to the multisource environment, the new ITISP suppliers were not able to report their status related to contractual requirements (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, and as of March 2020, the suppliers were still not meeting the minimum requirement of this SLA.

Difficulties encountered by the suppliers during the transition to the multisource environment led to suppliers not being able to initially meet all the contractual requirements. In 2018, VITA made the decision to classify the security and vulnerability patching related requirements as key measures to allow the suppliers time to implement their processes and reporting systems. Although key measures have contractual implications, there are no financial credits associated with the failure to meet a key measure. In August 2020, VITA promoted the security and vulnerability patching requirements to critical service levels, which can have financial credits applied when a supplier fails to meet the minimum requirements.

If a supplier is not installing security and vulnerability patches, an agency would first need to determine if the ITISP suppliers support the related application or system. If the ITISP do not support the application, it is the individual agency's responsibility to install the required patches. However, VITA does not maintain a master list of supported applications for agencies to check for validation. VITA should continue to work with the ITISP suppliers to prepare a detailed listing of all applications or systems that are supported under the current contracts.

To ensure all agencies that rely on the ITISP services comply with the Security Standard, VITA should ensure ITISP suppliers meet all contractual requirements. 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 of noncompliance with the Security Standard. If VITA determines a supplier is not meeting a requirement that has Security Standard implications, VITA should communicate with the affected agencies and provide guidance on what the agencies can do to mitigate the risk while the suppliers work to meet the requirements of the contract.

AUDIT SCOPE OVERVIEW

VITA is the Commonwealth's consolidated information technology agency. The responsibilities of VITA include the governance of the Commonwealth's information security programs, the operation of the IT infrastructure, the governance of IT investments, and the procurement of technology for VITA and other state agencies.

In December 2018, VITA transitioned the Commonwealth's IT infrastructure from a single supplier to a multisource environment. From 2005 to 2018, Northrup Grumman managed the Commonwealth's infrastructure, which includes data centers, networks, servers, routers, email, voice, data, security, mainframe, and personal computing services. In May 2018, VITA announced that it was terminating IT infrastructure services with Northrop Grumman. In its place, VITA implemented a new infrastructure environment that featured a multisource service integrator (MSI) and seven suppliers with shorter-term contracts.

Our audit focused on VITA's contract procurement, contract management, and billing business cycles. We placed specific emphasis on the contract procurement and management of the MSI and multisource suppliers.

Contracts

In August 2018, Science Applications International Corporation assumed the role of the MSI. The MSI's role is to coordinate and monitor the activities of the other suppliers, as well as to be the main resource for interaction with VITA and executive branch agencies. In December 2018, the other suppliers began providing services which include:

IT Infrastructure Suppliers and Services

Supplier	Service
Atos	Managed Security
Iron Bow	End-User Services
Perspecta	Mainframe
Tempus Nova	Messaging
Unisys	Server/Storage/Data Center
Verizon	Data/Voice Network
Xerox	Print Services

Our testing of VITA's procurement of the multisource contracts consisted of testing compliance with VITA's policies and procedures and statewide procurement rules. In addition to the multisource contracts, our testing included a sample of statewide IT contracts, which VITA procured during the period July 1,2017, through December 31, 2018. Other state agencies can utilize these statewide IT contracts for the purchase of IT and telecommunications goods and services.

Our audit also included testing of VITA's contract management for the period of January 1, 2019, through March 31, 2020. VITA and the MSI monitor the suppliers' contractual requirements, including deliverables and service level agreements, which are established in the contracts. Our testing of contract management consisted of contracts procured with the MSI, as well as the multisource suppliers.

Billing

VITA maintains three main repositories of data for billing purposes: IT goods and service asset data, mainframe data, and telecommunications data. As of July 1, 2019, VITA invoices its customers using three separate billing systems:

- Information Technology Financial Management (ITFM) system for comprehensive IT goods and services, miscellaneous services, and mainframe services;

- Voice and Data Networking (VDN) system for managed routers, wide area network, unified communications as a service, and executive teleconferencing services; and

- Telecommunications Expense Management and Billing Solution (TEBS) for local telecommunications services, broadband, and non-executive telecommunication services.

The MSI manages ITFM billing, with oversight and approval by VITA. VITA manages the TEBS billing for telecommunications services. Prior to July 1, 2019, the VDN billing was included in the TEBS system. Between July 1, 2019, and December 31, 2019, VITA managed the VDN billing separately while transitioning billing to the MSI. As of January 1, 2020, the MSI manages VDN billing within the ITFM tool. Our testing included monthly ITFM bills between July 1, 2019, and March 31, 2020, and TEBS bills between January 1, 2019, and March 31, 2020, to ensure processes were consistent with VITA's policies and procedures.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

January 29, 2021

The Honorable Ralph S. Northam
Governor of Virginia

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

We have audited the contract procurement business cycle of the **Virginia IT Agency** (VITA) for the period July 1, 2017, through December 31, 2018. In addition, we have audited the contract management and billing business cycles of VITA for the period January 1, 2019, through March 31, 2020. We conducted this performance audit in accordance with generally accepted government auditing standards. 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 Scope and Objectives

Our audit's primary objectives with regard to the contract procurement, contract management, and billing cycles were to review the adequacy of VITA's internal controls and test compliance with applicable laws, regulations, and contracts.

Audit Methodology

VITA's management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, and contracts. 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, as they relate to the audit objectives, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. 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 contracts as they pertain to our audit objectives.

Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of VITA's operations. We also tested details of transactions 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.

Conclusions

We noted one matter pertaining to contract management, involving internal control and its operation that requires management's attention and corrective action. This matter is described in the section entitled "Audit Findings and Recommendations." The results of our tests of compliance with applicable laws, regulations, and contracts, as they pertain to the audit objectives, disclosed no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

Exit Conference and Report Distribution

We discussed this report with management on February 4, 2021. Management's response to the finding 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/clj

COMMONWEALTH of VIRGINIA

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

Nelson P. Moe
Chief Information Officer
Email: cio@vita.virginia.gov

TDD VOICE -TEL. NO.
711

February 5, 2021

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 July 1, 2017, through March 31, 2020. We welcome assessment and recommendations from outside VITA and thank your staff for their time and effort on this audit report.

VITA's modernization of the Commonwealth's information technology (IT) infrastructure platform has made tremendous progress. When this audit period began, VITA was mired in disputes, in and out of court, with the previous single supplier. The Commonwealth had a decaying IT infrastructure environment, and the transition was troubled due to resistance from that single supplier. Over the nearly three-year period covered by the audit, VITA accomplished the fundamental transformation of moving from a single monolithic provider to a multi-supplier model. The multi-supplier model offers new technology, the flexibility and adaptability demanded by the pace of technological change and needed by VITA's client agencies, and significant cost savings to the Commonwealth over time.

Launching and maturing the multi-supplier model has required substantial effort from VITA, suppliers, and customer agencies over time. VITA had to adapt the transition plan to incorporate a caretaker period under Science Applications International Corporation (SAIC), transform VITA itself to meet the requirements of managing the multi-supplier model, work with suppliers to modernize the IT infrastructure and overcome technology "debt" that built up during latter years of the prior model, and build the governance and technological systems and processes that enable the multi-supplier model's success. By mid-2020, key objectives had been achieved, including:

- Development and finalization of operating level agreements among suppliers to reflect and support the shared effort and accountability needed in a multi-supplier model.
- Implementation of a contract deliverables and obligations tracking system (DOTS) by SAIC.
- Adoption of an operations and management focus on data analysis, enabling data-based reporting and decision-making and improving insight to measure and improve performance.
- Consistent supplier reporting against contractual service levels, and VITA holding suppliers accountable, including collecting invoice credits where their performance falls short.

At the same time, VITA, suppliers, and agencies have been working to achieve other essential strategic goals, such as launching new services, migration to cloud-based systems and services, and moving from the current Commonwealth Enterprise Solutions Center (CESC) data center to the new QTS data center.

This overall background and context is included not to dispute that work remains to be done but to describe how the enterprise environment has built a foundation for further progress, addressing outstanding needs, and optimizing current operations.

The audit brought one internal control matter to management attention – the need to ensure that all contractual requirements are met by infrastructure suppliers. VITA agrees that is essential to success, and VITA is focused on continuing the improvement to date in that area.

After the commencement of services by the suppliers in December 2018, standing up and maturing supplier performance reporting against contractual service levels took longer than initially hoped. The systems for reporting needed to be built under the multi-supplier model, and implementations and reporting were delayed by various factors.

In late 2019, VITA began enforcing contractual service level agreements (SLAs) and deliverables, including by collecting performance credits. (SLAs are categorized into Critical Service Levels and Key Measures. Performance credits are available for Critical Service Levels, subject to certain contractual and practical limits. SLAs that are not associated with performance credits are still reported and reviewed monthly, and the suppliers are expected to perform according to the service level requirements.) As of March 2020 supplier performance data, VITA and the MSI had 231 out of the 248 SLAs reporting, with consistent improvement in the accuracy of the measures and reports.

The infrastructure contracts allow VITA to change the categorization of SLAs on a quarterly basis, with 45 days of notice, and VITA is regularly leveraging this contractual mechanism to

drive supplier focus on SLAs of particular interest. VITA also has leveraged other mechanisms for improving supplier performance, such as agreement on specific service improvement plans.

Within the general area of ensuring contractual requirements are met, the audit focused on the need to ensure that IT infrastructure platform operations comply with the Commonwealth's security standard and highlighted two instances where work remains to be completed, namely: (i) ensuring that security-relevant software updates are applied in a timely manner to all devices, and clarifying responsibilities for applying updates; and (ii) providing agencies with direct access to the centralized security incident and event management tool that collects audit log information. VITA is working to resolve these issues in ways that were not possible without the foundation provided by the progress over the last few years.

VITA promoted the Vulnerability and Patching SLA to a Critical Service Level, effective August 2020 for the multisourcing service integrator (MSI) and November 2020 for service tower suppliers (STSs), to ensure increased attention on the performance under this SLA and improved presentation of related data. Promotion and the availability of a financial performance credit encourages the suppliers to address the SLA more aggressively. VITA is also using improvement plans to address patching performance. Below is a summary view of the recent supplier performance on this SLA:

Tower	CSL/KM Title	SLA Type	Share Type	Expected	Minimum	VITA November Decision	VITA November Comments	VITA October Decision	VITA September Decision
MSI	MSI 2.3.4 Security and Vulnerability Patching (CSL)	CSL	R	99.50%	99.00%	PASS	99.98%	PASS	PASS
Security	MSS 2.3.4 Security and Vulnerability Patching (CSL)	CSL	R	99.50%	99.00%	DEFAULT	0.83%	DEFAULT	PASS
Server Storage Data Center	SSDC 2.3.4 Security and Vulnerability Patching (CSL)	CSL	R	99.50%	99.00%	DEFAULT	92.62%	PASS	DEFAULT
Managed Print	MPS 2.3.4 Security and Vulnerability Patching (CSL)	CSL	R	99.50%	99.00%	PASS	100.00%	PASS	PASS - No Data to Report
End User Support	EUS 2.3.4 Security and Vulnerability Patching (CSL)	CSL	R	99.50%	99.00%	SLA REMEDIATION PLAN	97.02%	DEFAULT	DEFAULT
Voice Data Network	VDN 2.3.4 Security and Vulnerability Patching (CSL)	CSL	R	99.50%	99.00%	DEFAULT	86.68%	DEFAULT	DEFAULT

As this summary reflects, VITA actively tracks patching and reporting by supplier and finds them in default of service levels when the targets are not reached.

VITA continues to see trends of improvements in patching performance following the steps that we have taken. It is important to note that many patches are being applied successfully on an ongoing basis on both workstation and server levels. Starting in the October/November 2020 timeframe, vulnerability reports also confirm that the patching enterprise-wide has improved. VITA is committed to driving further improved performance.

VITA also is working with the suppliers to finalize lists of software being patched to ensure that customer agencies know what applications they are responsible for updating. VITA stands ready to work with customer agencies on how to address systems or applications that are not updated by the infrastructure suppliers.

With respect to security generally, VITA certainly agrees with the necessity of compliance with the Commonwealth's standards. The introduction of a managed-security services supplier, Atos, as part of the multi-supplier model, is helping to ensure that VITA has a full picture of where vulnerabilities and risks exist, as well as identify any actions for mitigation.

Aside from reviews triggered by specific issues (including reporting from tools and from customer agencies), VITA uses two processes to check for compliance with security standards: one during implementation of services and one for maintaining operations. For implementation, VITA has an architecture review process that requires suppliers to detail how their systems will be designed and whether there are any issues concerning compliance with security standards. VITA reviews the designs carefully, including looking for implementation issues that would result in non-compliance with the standards. The operational process then uses the security toolsets provided by Atos – each service has a corresponding security tool that provides data regarding compliance. Reported deviations go to the MSI for remediation with the tower supplier. The MSI's role includes reporting on the status to VITA and the suppliers. Security personnel in VITA monitor the issues for progress, and VITA's risk management team considers, generates, and tracks risk alerts that may be needed if issues go unresolved over time. Through these processes, VITA monitors for security standard compliance on an ongoing basis.

VITA will work diligently to make further progress on the matter noted in the audit. Thank you again for the review, and we look forward to working with you in the future.

Sincerely,

Nelson P. Moe

Nelson P. Moe

cc (by email): Noah Johnson, APA

Virginia IT Agency

As of March 31, 2020

Nelson P. Moe
Chief Information Officer

Michael Watson
Chief Information Security Officer

Jonathan Ozovek
Chief Operating Officer

Dan Wolf
Chief Administrative Officer