VIRGINIA IT AGENCY

Cybersecurity Staffing Plan

Virginia Information Technologies Agency

vita.virginia.gov December 2021

TABLE OF CONTENTS

INTRODUCTION

VITA provides information technology (IT) infrastructure services to the Commonwealth's 65 executive branch state agencies and the workforce of over 55,000 state employees, equipping and empowering the agency's colleagues to serve Virginia's 8.6 million residents. Cybersecurity governance is a critical part of VITA's statutory responsibilities. *See, e.g.*, Va. Code § 2.2-2009.

The 2021 organizational review of VITA by the Joint Legislative Audit & Review Commission (JLARC), available at http://jlarc.virginia.gov/landing-2021-vita-organizational-structure-and-staffing.asp, contained the following recommendation:

> *The Virginia Information Technologies Agency (VITA) should develop a plan to fully staff its Commonwealth Security and Risk Management group to meet its statutory responsibilities. The plan should specify the number of additional staff needed in the group to carry out its security, risk management, and enterprise architecture functions, and the roles these staff would fill. VITA should provide the plan to the Joint Legislative Audit and Review Commission, Senate Finance and Appropriations Committee, and House Appropriations Committee by December 15, 2021.*

The VITA team agrees that growing the cybersecurity workforce is necessary and appreciates the opportunity to share more information on this critical subject.

THE COMMONWEALTH'S CYBERSECURITY PROGRAM

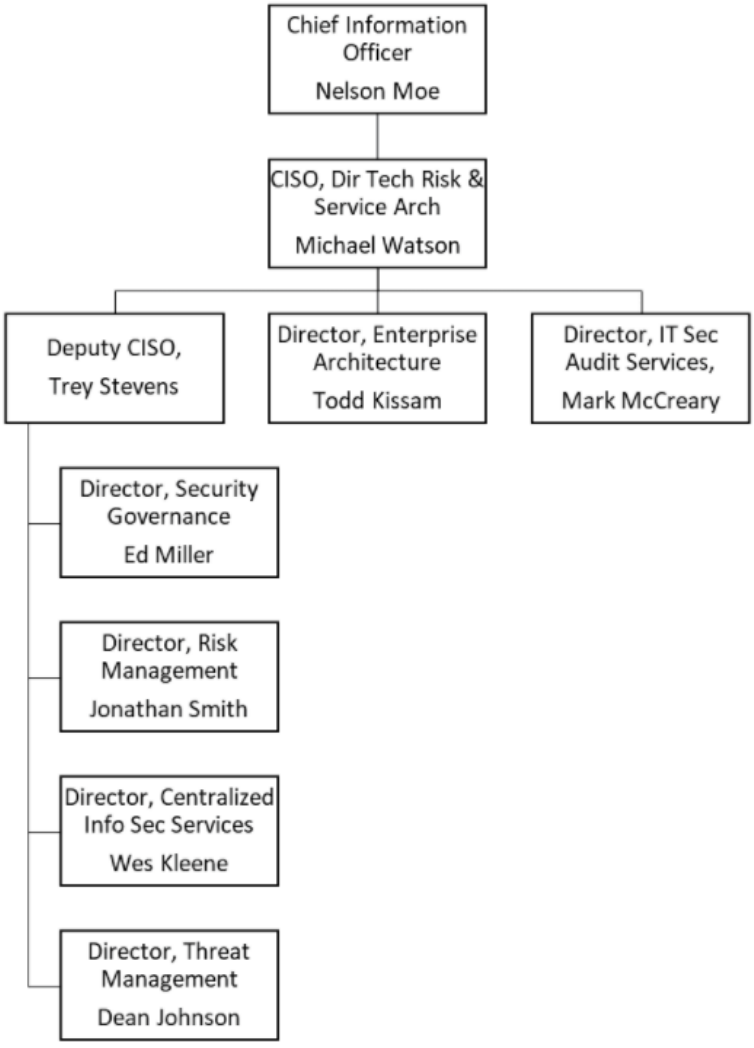
STRUCTURE

The Commonwealth's cybersecurity program is divided into four main areas:

- governance and oversight,
- risk management,
- threat management, and
- architecture.

Governance outlines the minimum standards the Commonwealth must meet to provide a secure and reliable operating environment for systems and data. Risk management maintains the target risk thresholds the Commonwealth has set to operate within. Architecture sets the operating parameters and design for technology in use in the environment. Threat management responds to threats and compromises to the environment. These areas are designed to support business units during their development, implementation and operation of technology.

As shown in the organizational chart at the right, VITA's Commonwealth Security and Risk Management (CSRM) group has directorates for each of the above four areas, as well as two other directorates: IT security auditing and centralized information security officer (ISO) services.



THE GROWING THREAT AND NEED FOR INCREASED CYBERSECURITY STAFFING

Over the past several years, multiple factors have coalesced to create an urgent need for increased staffing in CSRM. First, technology is now integral to the business and policy of government. Today, every project is a technology project, and every policy has technology dimensions. Second, the transition to the multisupplier model and the widespread use of software-as-a-service (SaaS) and other cloud services results in more suppliers and services to assess and manage. Third, the move to remote and hybrid work heightens exposure to cyberattacks. Fourth, at the same time that demand and complexity are increasing, the threat and impact of cyberattacks are rising, too. *See, e.g.*, JLARC 2021 organizational review of VITA at 24; VITA's Ransomware Study Report (January 2021) at 7-8.

Due to the increasing threats from malicious parties, Virginia is at a critical juncture for the cybersecurity program. Successful attacks on public bodies and critical infrastructure impact both the function of government and the lives of citizens. Additional staff is necessary for prevention of and response to the constant cyberattacks on the Commonwealth's IT environment. Absent adequate staffing, further preventable compromises can be expected.

WORKLOAD AND STAFFING IMPACTS BY AREA

The Commonwealth Security and Risk Management (CSRM) group is beginning to experience specific impacts of inadequate staffing in each area of CSRM:

Governance

The Commonwealth does not currently have adequate security standards for cloud technology. Cloud services use a different security model than the Commonwealth has used to date. In order to maintain an enterprise that securely operates with all cloud service solutions, significant updates to Commonwealth policies, standards, and guidelines are needed.

Identity and access management is a core framework component of cybersecurity. Additional requirements and enforcement of security measures such as multi-factor authentication must be implemented.

Operational technology (OT) security requirements need to be developed. OT refers to hardware and software that monitors and/or controls physical systems and assets (such as control systems and internet of things devices). The threat landscape is trending toward more of these attacks, and the state's ability to identify and recover from such an attack has been more limited than attacks on traditional computing devices. Presently there are significant gaps in securing OT systems and devices.

An updated security strategy must be developed and implemented in the Commonwealth's environment, using zero trust framework architecture. Traditional, perimeter-based security is increasingly inadequate to monitor and manage risk in a world that features extensive remote

access and cloud-based services. The zero trust framework changes how enterprises secure their environments from securing a perimeter to enforcing the identity of each connection, user, and asset throughout the network to prevent breaches. Zero trust tools and services provide capabilities to baseline normal behavior and automate prevention measures when deviations are seen. Implementation of a zero trust framework security architecture will require a strong coordination between VITA and agencies in order to be successful. The first step is to make sure the right governance documents are in place to define and direct responsible parties.

Analysis and reporting on the state of agency information security program continues to run behind schedule.

Enterprise/Security Architecture

To accommodate the new network technology being introduced for cloud services, the new Commonwealth data center, and agency locations, an updated network security model is needed. The architecture used in the Commonwealth Enterprise Solutions Center (CESC) does not translate well to the move to the hybrid cloud model in use today. Yet, at present, the team is struggling to keep up with the increased demand from agencies and the enterprise, resulting in implementation of technology without assurance of security adequate to mitigate risk to targeted levels.

Another responsibility of the architects is to participate in the procurement process for new technology purchases of sufficient size. VITA's release of requests for proposals (RFPs) to replace current IT infrastructure services will qualify. These RFPs are expected to occur over the next few years for most IT infrastructure services, including security, network, endpoint, and server services. Dedicated time must be allocated by the team for each procurement.

A backlog of third-party security technical reviews exists, due to the increased demand. Agency requests have more than doubled, and this year the agency employs a single full-time employee to handle security reviews for over 140 different vendors.

The team has been unable to engage in needed evaluations, for security gaps and design issues, of as-built and agency system and technology designs.

As of mid-November, in 2021 there have been 386 new security exception requests for gaps identified in the Commonwealth of Virginia (COV) security architecture established by security standards. In addition to those new exception requests, there have also been 138 extensions filed for existing requests. Security exceptions are meant to be short term (not to exceed one year) while a secure solution is designed and implemented. The architecture team should be able to help the agencies design solutions to mitigate these issues instead of maintaining them on the network. Current staff must handle three of these each day in order to keep up with current rates. The target workload should be approximately five per week, meaning that the current workload is triple what each person should be handling.

In addition to addressing the existing gaps, the architecture team provides the technical expertise for new technology and products to introduce into the Commonwealth environment. The current staffing levels have not allowed the architects to be proactive in either suggesting new technologies or preparing the environment for new requested technologies.

Threat Management

The number of new threats continues to increase year after year. 2021 is on pace to end with more than 430 incidents. Security attacks have become more creative and complex, resulting in a more difficult investigation process. Cloud services have spread data and technology out across several platforms. The continued increase in technology and services means the scope of what needs to be protected has grown.

Simultaneously, the amount of time to resolve incidents is longer than it used to be. In 2019, the average number of days an incident remained open was 34 days. In 2020, that increased to 57 days. 2021 is averaging 51 days so far, a 42% increase from 2019.

As noted above, ransomware and other cyber extortion and the security of cyber physical systems are areas of concern, both with significant potential for high impact, high loss, and difficult recovery. In addition to such direct threats to Commonwealth systems, supply chain threats (where a compromise of a supplier enables an attack on that supplier's customers) are a significant risk. Inadequate staffing threatens the ability to investigate and respond to such threats, as well as threats to third-party systems hosting Commonwealth data, which is increasingly common with greater use of software-as-a-service (SaaS) and cloud hosting.

Vulnerabilities and configuration issues are lingering in the Commonwealth's environment for excessive periods. There are more than a thousand publicly-accessible security vulnerabilities impacting the technology used in the environment. At current staffing levels, it is not possible to identify and mitigate each and every instance. There has been a recent uptick in exploitation of these vulnerabilities, with additional increases expected.

Insufficient staffing levels also result in a lack of time spent on analyzing available threat intelligence. The distilled analysis can be used to proactively predict and prevent attacks that are currently being experienced today. This analysis would also be used to lower the amount of time it takes for a successful attack to be discovered, resulting in lesser impact to the Commonwealth.

Risk Management

The primary role for this team is to understand the amount of risk the Commonwealth assumes via the use of technology, whether within the Commonwealth's network or via a third party. This team reviews hundreds of contracts and security plans for Commonwealth systems to ensure risk is mitigated as much as possible. The increase in technology use over the last few years has resulted in the team falling further behind on risk analysis and mitigation.

The team also maintains the security risk posture for the enterprise. There are over 4,200 security findings in the environment driven by known issues at the agencies. At the current staffing level

of four, the team is effectively unable to work with agencies to come up with the risk treatment plans needed to decrease our risk.

Through November 14, 2021, 2,648 risk findings have been recorded. If the current pace continues through the end of the year, there will be a 26% increase from 2020. With current staffing levels, only 10% of these recorded risks have been successfully closed. Risks also remain in the environment much longer than they should, with the backlog reaching 11 months if the pace continues. These risk management shortcomings result in significant financial and reputational risk to the Commonwealth. Additionally, they have the potential to impact cyber insurance coverage because the coverage is dependent on the Commonwealth addressing cyber risks in a timely fashion.

Centralized Security Services

The centralized services cover over 638 applications, 1,467 business processes, and over 600 identified security gaps (*i.e.*, instances of exceptions or deviations from Commonwealth security standards). The number of such gaps has been consistently larger than expected and additional assistance is needed to fill these gaps at the agencies.

CURRENT STAFFING SUMMARY

Out of VITA's 210 current employees, 36 are in Commonwealth Security and Risk Management (CSRM), along with three full-time contractors. Tenure in CSRM ranges from two months to 41 years.

Six CSRM positions are in active recruitments (one Security Architect, one Security Architecture Manager, one Info Tech Security Auditor, two Enterprise Architects, and one Incident Response Specialist).

The job classifications and pay bands of CSRM employees are as follows:

Pay Band	Employees
5	4
6	18
7	13
8	1

Titles/Codes	Employees
Audit Services Manager III	1
Auditor II	4
Info Technology Manager II	4
Info Technology Manager III	1
Info Technology Specialist III	18
Info Technology Specialist IV	8

ADDITIONAL STAFFING NEEDED

VITA's plan for additional cybersecurity staffing has two phases. The first phase will address the immediate staffing gap, which is either unnecessarily increasing cost to the Commonwealth or putting the Commonwealth at significant risk for a cyber-related compromise. The second phase will add the staff needed to support the security and architecture metrics measured.

In the table below, each directorate's current number of positions and the number of positions identified as needed as part of this plan have been identified.

	Governance	Risk	Threat	Architecture	ISO Services	Audit
Current positions	6	5	5	10	6	6
Additional proposed positions						
*** Phase 1**	2	2	3	8	1	
*** Phase 2**		2	0	4		
Total	8	9	8	22	7	6

Phase 1

- Governance would add one information insurance analyst and one IT compliance analyst.
- Risk Management would add two cyber risk analysts.
- Threat Management would add one incident response analyst and two cyber threat management and exploit specialists.

- Centralized ISO Services would add one information security officer.
- Architecture would add:
    - One technical architecture manager
    - Three technical architect (two EA and one security)
    - One security architect
    - One governance architecture manager, and
    - One governance enterprise architect

Phase 2

- Risk Management would add two cyber risk analysts.
- Architecture would add one enterprise architect, one technical architect, and two security architects.

CONCLUSION

Investment in security personnel should directly correlate with increased technology use and needs. Investment as described in this plan will enable the Commonwealth Security and Risk Management group to catch up to the current level of requests and demand, as well as position them for at least the next few years of technology development and investment.

The cybersecurity landscape no doubt will continue to evolve along with the technology in use. New threats and challenges will arise, but having the staff in place to address cybersecurity issues proactively before crises occur is a more effective and cost-efficient way to address cybersecurity. And not everything is new and unknown -- cybersecurity problems and compromises often relate to known security gaps. Investment as described in this plan will take time to implement. Cybersecurity personnel are in high demand, and recruitment and hiring take time, but it is critical to begin that work now. Sufficient staffing will better protect the Commonwealth's critical infrastructure and valuable data assets, and investment in prevention through the cybersecurity workforce is a better and more efficient use of public resources than spending on response and recovery to address incidents after they occur.