VIRGINIA IT AGENCY

2025 Network Infrastructure Report

Virginia Information Technologies Agency

vita.virginia.gov

November 2025

THIS REPORT

The Virginia IT Agency (VITA) is submitting the network infrastructure report, pursuant to Item 79(E) of the 2024 Appropriation Act, which provides:

> The Virginia Information Technologies Agency shall provide a network infrastructure report to the House Appropriations Committee, Senate Finance and Appropriations Committee, and Joint Legislative Audit and Review Commission by November 1 of each year. The report shall indicate whether the Commonwealth's network infrastructure is adequate to meet the needs of state agencies, and if not, identify any needed upgrades. For each network infrastructure upgrade identified, the report shall specify the estimated cost and whether the upgrade is to the portion of the network maintained by the Virginia Information Technologies Agency or another state agency.

This report covers December 2024 to October 2025. This report details the progress since the last report and the network infrastructure needs of state agencies. VITA thanks policymakers for this opportunity to report on this important subject.

INTRODUCTION

VITA provides information technology (IT) infrastructure services to the Commonwealth's 67 executive branch agencies and a workforce of over 65,000 state employees, equipping and empowering executive branch agencies to serve Virginia's 8.6 million residents. The large Commonwealth network not only provides agency services but also segregates traffic for each agency to provide the necessary security and privacy requirements.

Network infrastructure forms the foundation for almost all government interactions with Virginians. But a network is not viable or useful if it does not enable convenient, reliable, and secure customer usage. Network infrastructure therefore includes not only the network circuits and related hardware but also the software that helps run and maintain the Commonwealth's network and the security services and controls that provide a secure platform and guard against threats, making it possible both for agencies to protect their systems and data and for users to access those resources. Accordingly, this report includes discussion of network, security, and cloud technologies and initiatives that improve network redundancy and resiliency or that fulfill essential network security functions.

This year's network report describes multiple initiatives that have bolstered network resiliency, redundancy, reliability and overall performance. These efforts include voice and data modernization, building a zero-trust security framework, private and public cloud migrations, and performance and network monitoring.

REPORT

Modernization is essential to foster an agile, secure, and high performing IT landscape. Network modernization efforts improve efficiency and effectiveness of communication networks, including opportunities to lower costs, and ensure security and reliability of data and voice services.

Voice Service Maturation

Microsoft Teams Enterprise Voice is a service offering aimed at reducing cost for voice services. It allows users with Office 365 G5 licensing to make and receive phone calls on their Microsoft Teams client for desktop and mobile. No physical phone is required. Through this service, agencies may reduce their monthly telecommunications expenses compared to current costs for voice services.

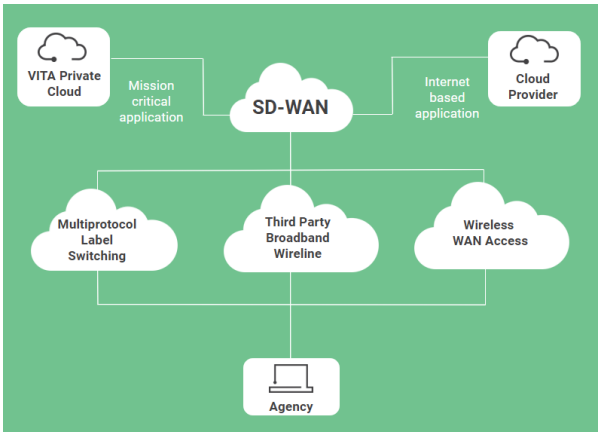
Managed Software Defined-Wide Area Network (SD-WAN)

VITA, our supplier, and agency partners have made tremendous progress in implementing SD-WAN capability for every executive branch agency. SD-WAN allows organizations to leverage many network transportation methods to securely connect users to applications. SD-WAN software responds to real-time network conditions, integrates intelligence at the network edge to identify traffic patterns or bottlenecks, and directs applications and services along paths that support their unique performance and security needs, offering improved agility and control.

What is SD-WAN? *SD-WAN stands for Software-Defined Wide Area Network. SD-WAN uses software to route network traffic to allow agencies to efficiently manage and optimize their network operations*

SD-WAN brings several benefits to agencies, including enhanced application reliability, capacity, and network security, all without sacrificing performance. When implemented together with adding a lower-cost broadband circuit or other connections, SD-WAN can result in significantly increased bandwidth and performance.

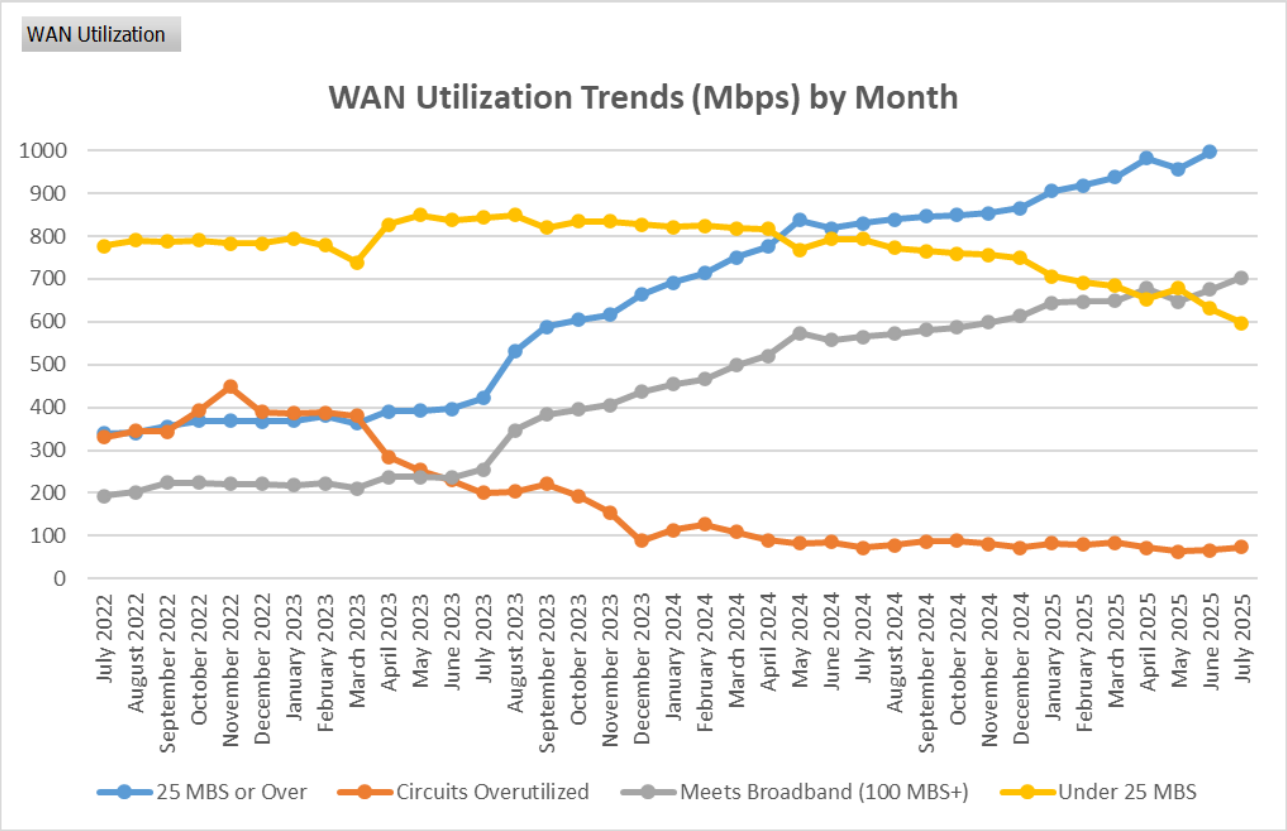
Table 1. Managed SD-WAN



VITA and other state agencies have taken advantage of this technology with circuit upgrades, wireless access devices and broadband circuit installations. Currently 1,172 out of 1,181 (99%) of sites have had SD-WAN installed and 611 (51.7%) of these sites have a secondary broadband circuit installed as well.

Network utilization reports show that this modernization has had a real effect. There has been a significant reduction in reports of congested (or overutilized) network circuits (known as "hot site reports") decreasing from 391 in February 2023 to 75 in July 2025 – an 81% reduction. (See Appendix A for the August 2024 hot site list, together with the costs to bring those sites up to the recommended circuit bandwidth.)

To take full advantage of SD-WAN, agencies may require funding to acquire broadband circuits or other connections that enable network optimization. As the project moves forward, there may be cases where construction costs are necessary to provide modern circuits to agency facilities.



Capital Ring Upgrade

VITA has canceled the planned upgrade to Dense Wavelength Division Multiplexing (DWDM). Instead, the agency will leverage existing technology and investment in Software-Defined Wide Area Networking (SD-WAN), which offers both redundancy and increased bandwidth capacity at a significantly lower cost.

Cloud Connectivity Strategy

Since VITA has committed to a CISCO based SD-WAN technology and implemented it at over 1100 sites, the next step is to create a standard network infrastructure taking full

advantage of SD-WAN technology. VITA is utilizing a SD-WAN hub within each cloud tenant to enable simple access for an agency to any cloud tenant, including cloud to cloud. SD-WAN hubs enable encrypted dynamic routing to any hub, thus immediate connectivity. Additionally, VITA is enabling Software Defined Interconnect (SDI) technology to replace Secure Cloud Interchange (SCI) connections. SDI enables all agencies to take advantage of an established connection and eliminates the need for individual connections while sharing bandwidth.

Implementing these changes enables agency sites to easily access the multi cloud tenants and decreases infrastructure build-out timelines for agency to cloud tenant connection to days versus multiple weeks.

Managed Security Services RFP

VITA is in the process of evaluating responses for Managed Security Services Request For Proposal (RFP). This RFP is part of VITA's sourcing efforts to deliver both traditional Information Technology security services such as workstation and server anti-virus, network firewalls, and intrusion detection systems as well as newer technologies related to Cloud security and Zero Trust components.

Examples of those newer technologies include Cloud Native Application Protection Platform (CNAPP) which provides a comprehensive view for the security posture of the various managed cloud computing environments, Microsegmentation which creates very small and isolated network segments thus limiting the impact of security breaches within specific segments, and Secure Service Edge for providing a unified, cloud-based, set of security controls.

Building a Zero Trust Security Framework

Today's state government network is a complex environment, featuring over 1,700 sites and data and applications increasingly transitioning to the cloud. Robust cybersecurity for the Commonwealth's network and data is an essential part of providing network infrastructure services.

The Commonwealth's security posture will be enhanced by moving to a zero-trust framework. Benefits of zero trust include a reduction of cyber risk by reducing the network attack surface, limiting the ability of attackers to expand out from an initially compromised system, and operational efficiencies for policy management.

Zero trust does not refer to any single security technology. Zero trust is a security approach or framework that does not automatically trust any user or device inside a network; instead, users and devices are continuously verified. These best practices approach will protect the Commonwealth's IT resources from the next generation of cyber threats and provide a secure architecture and best practices for cloud, artificial intelligence, and third-party services regardless of what network a system is on. Improvements to remote access, content filtering, privileged access management, identity

and access management and multi-factor authentication all play a pivotal role in establishing a zero-trust environment.

VITA is working to update the Commonwealth security model to zero trust. Specific improvements along the road to zero trust are discussed below.

Identity, Credential and Access Management

A network is not useful unless people can access the right resources on the network. Identity, Credential and Access management (ICAM) is a core foundational component of Zero Trust (ZT) that can involve multiple technologies and processes and aims to help the right people and devices access the right resources at the right time.

Under ICAM, Single Sign-on (SSO) relieves the burden of needing to remember passwords for multiple applications and streamlines access. SSO also helps the enterprise monitor access and speed deployment of new applications.

Okta is the platform that supports the Commonwealth's enterprise single sign-on service. Okta enables multi-factor authentication (MFA) for all users and systems, which has increased from over 800 to over 1000 application and system integration instances. VITA SSO is configured to support both internal state government users and external users, such as local government. VITA continues to improve this environment to support agency requirements while increasing the Commonwealth's security posture.

This year, VITA enforced MFA for all non-COV network connections, along with strict inactivity session timeouts. VITA has also enabled and deployed phishing resistant MFA, which includes Okta Verify for Mobile, Okta FastPass for Windows, and YubiKeys with FIDO2. For Okta FastPass, user verification has been enforced as an additional security control.

Following Industry best practices, VITA incorporated the concept of decentralized digital identity by integration more than 130 Virginia school division identity providers (IDPs) with just-in-time (JIT) provisioning to enable access to DOE's Virginia's Visualization and Analytics Solution (VVAAS).

VITA updated the Okta integration catalog item to streamline the onboarding and integration of agency applications, while providing additional security review to ensure applications are authorized for use in association with COVRAMP requirements.

SailPoint Identity Security Cloud is a modern identity security solution that provides a centralized way to see and control every user's access to resources across hybrid IT environments, while ensuring regulatory compliance. Implementing SailPoint Identity Security Cloud as the executive branch identity governance solution allows agencies to view access roles and policies for all users and objects across the Commonwealth's complex environments. Identity Security Cloud automates access provisioning, monitors for inappropriate access, and enforces policies based on roles and activities.

Key Commonwealth systems (such as Cardinal) have been integrated with ICAM technologies to enhance the data quality and consistency of employee identities, accounts, and attributes.

VITA is deploying a new password management service called CyberArk Workforce Password Manager (WPM). CyberArk WPM is designed to address the challenges organizations face in securing and managing passwords, especially for business applications that rely on traditional username and password credentials. CyberArk WPM provides enhanced security, improved control and visibility, simplified access and users experience, and integrates with our SSO platform.

VITA continues to pursue MFA at login and has completed initial testing with Okta Device Access. VITA is actively coordinating with Tax as a key stakeholder to conduct further testing to ensure that the solution will meet agency requirements.

PRIVATE & PUBLIC CLOUD SERVICES

People referring to "the cloud" typically mean the "public cloud," where external cloud providers (Amazon Web Services, Microsoft, etc.) deliver cloud resources (such as storage and computing power) as a fully managed service. Public cloud services are provided to agencies through the COV Cloud program. Private cloud refers to situations in which a single organization controls the underlying infrastructure to deliver the IT resources in a cloud-like manner, which has been made possible for the Commonwealth thanks to virtualization and the migration of the Commonwealth's datacenter to the QTS datacenter in Eastern Henrico. Both public and private cloud improvements are discussed below.

COV Cloud

The Commonwealth continues to transition workloads to the cloud. In order to realize the benefits of the cloud, VITA is modernizing cloud service management and executing a strategy to transition to a "consumption" based model, instead of the previous "resource unit" model. This change, which transitions customers away from paying for resources, whether used or not, to paying for only what is consumed, positions the Commonwealth to fully leverage cloud capabilities, including cloud native services, solution flexibility, scalability, and more granular and controlled costs.

For overall management, VITA has implemented the CloudScend tool, which provides a consolidated view of services across multiple cloud platforms and enables automated provisioning of cloud resources, agency self-service and management, improved cloud billing information, and cloud resource utilization and planning. CloudScend replaces "resource unit" billing with consumption-based billing, thus bringing true cloud advantages to fruition.

To ensure competition and value from cloud services, VITA released a request for proposals (RFP) to transform how public cloud services are provided in the Commonwealth, covering the multi-cloud environments currently operated or requested by agencies. VITA is working to transition from a single managed cloud services (MCS) provider supporting all cloud environments to a model with additional supplier diversity (ideally a different provider managing each cloud). The RFP was awarded for management of the Azure cloud environment in October 2024 and services were

transitioned in March 2025. The new Azure supplier has begun remediation and modernization and is on track to releasing the service that meets VITA Rules by Fall 2025. Amazon Web Services (AWS) and Oracle cloud environments remain with the current supplier.

DISASTER RECOVERY AS A SERVICE (DRAAS)

VITA commenced a project to refresh and modernize its Disaster Recovery (DR) Service. Today the service consists of an 'all or nothing' approach when declaring a disaster. Meaning all subscribers are switched to the DR or none are. The 'bubble' approach does not support individual agency disaster scenarios. Thus, VITA is working with its suppliers to create a disaster recovery service that is agency/application based and is recovered in its cloud tenant versus the Ashburn DR data center. The project is the first move in eliminating the Ashburn site and moving its functions to the VITA clouds.

Uninterruptible Power Supply (UPS) Service

Past network reports also have discussed the importance of reliable power to network services. In June 2024, VITA released a new offering of a simple rack uninterruptible power supply (UPS) service. The goal is to eliminate urgent service tickets and equipment repairs in the event of power outages, thus minimizing damaged hardware and increasing availability at affected locations.

UPGRADES AND ASSOCIATED INVESTMENTS NEEDED

While VITA is making crucial improvements to ensure the reliability and performance of the Commonwealth's network infrastructure, further upgrade work would enhance these efforts. Investments needed encompass upgraded network circuits, expanding redundant networking, circuit modernization, strengthening network access and security, facilitating private and public cloud migrations, streamlining data center elimination, optimizing disaster recovery, bolstering ransomware protection, and elevating performance monitoring.

Upgrading network circuits for agency sites

Additional funding would enable agencies to take full advantage of the capabilities of SD-WAN by procuring broadband circuits or other lower-cost, higher-capacity connections, enabling network traffic optimization through SD-WAN. Current network improvement efforts may identify locations where construction costs are necessary to provide modern circuits to an agency facility.

Where network circuit utilization is showing oversaturation, and where current circuit size does not meet VITA's recommended network bandwidth-per-user standard, upgrading is

recommended to reduce congestion and to meet the standard. (Appendix A includes estimated costs for upgrading remaining congested circuits.) VITA is implementing SD-WAN at every agency to leverage cost efficient broadband circuitry compared to MPLS circuits. As stated, as each agency and location are evaluated for bandwidth upgrades, agencies can choose from broadband, MPLS, or wireless enhancements. Some agencies may need construction funding to extend service to specific locations.

Expanding redundant networking

Redundant network connections provide multiple paths for traffic. This ensures an organization's uninterrupted online presence, even in the event of a failure of one connection or part of a network. Redundant network connections also can boost performance through improved traffic routing and management. For critical sites identified to VITA, such as hospitals and traffic operations centers, VITA and agencies have already worked together to ensure redundant network connections. This is accomplished by utilizing two or more circuits or implementing broadband backup to traditional circuits. The definition of critical sites could be broadened to include:

1. Every agency headquarters, given that all agencies depend on the network for their business, and
2. Every site where agencies and members of the public interact in-person in a way that cannot be fully replaced by online transactions, such as Department of Motor Vehicles offices.

VITA recommends agencies review the locations in need of redundant network connections and consider adding redundancy if appropriate. For example, in light of delay in moving the last couple of critical agency applications off the mainframe, VITA's RFP for the 2024 mainframe contract added requirements for circuit redundancy and diversity.

Circuit modernization

In line with initiatives such as SD-WAN, overutilization of circuits should be fully remediated. SD-WAN can decide the best route (circuit) to be used, but where one of the circuits fails, the remaining circuit may not be able to accommodate the business workload. For example, a site may have had a T1 circuit (1 MB throughput) and then added, via SD-WAN, a 100 MB broadband circuit. If the broadband circuit fails, the T1 circuit does not have the necessary capacity to support the agency's business. Progress has been made through current network modernization efforts, but future investment in modernizing circuits should seek to ensure their capacity aligns with workloads. Priority should be given where outdated technologies reside (such as T1s), or where site location buildouts are needed, all within agency business support models.

Network access and security

Agencies' ability to take advantage of the many network access and security services that are being rolled out depends on agency planning and budgeting. For example, to enable authentication to external users for an application, new OKTA licenses and ongoing support must be part of the project.

On an enterprise level, VITA's ongoing efforts with zero trust implementation are based on organic growth of existing products and continued roll out of products such as SailPoint and Okta. Continued funding for these efforts is necessary to create enterprise services in these areas, but this investment does not necessarily increase Commonwealth spend – in many cases, the results of the modernization effort will reduce overall Commonwealth costs.

Additional implementation opportunities will be driven by tool replacements, new implementations of software, integration of new suppliers, and product updates that will enable a zero-trust model.

Private and public cloud services public cloud migrations

To continue migrating workloads to the public cloud, VITA needs to continue to reduce reliance on any physical data center and ensure a secure cloud architecture is in place.

Many security services – such as logging and data inspection, workload backups, application availability, and disaster recovery services – can be delivered within the public clouds, as outlined above. Although an investment by VITA, enterprise services such as SDI and SD-WAN will enable a lower cost to agencies for cloud adoption and usage.

As VITA continues to transform public cloud services in the Commonwealth, through initiatives such as the modernization of managed cloud services, it is imperative that VITA internalizes the necessary skills to not only oversee and govern the changing environments but to have the technical knowledge to own and lead the services going forward. Additional resources to serve as service owners as well as architects are needed for VITA to align these changing and expanding services with the agencies' vision.

Additionally, as agencies utilize services from the clouds, their need to migrate workloads may create resource requests.

Eliminate Secondary Data Center

Initiatives are in flight to eliminate the secondary data center and reduce footprint in the primary data center. The driver behind eliminating the secondary data center is the migration of servers to the cloud. Agency investment in application modernization and enabling cloud migrations may require additional funding. Projects to migrate the core infrastructure services within the primary data center will need to be engineered for cloud

failover as well. Additionally, plans to move backup services and other physical disaster recovery services from Ashburn needs to be executed.

Modernized Disaster Recovery

To modernize disaster recovery services, the Commonwealth must have the ability to failover to other production sites. These sites can include physical and/or public cloud data centers. This requires VITA to design and build a robust network infrastructure to provide resilient communications pathways to the alternative sites for use in case of a disaster declaration. VITA has commenced the project for a portion of its DR services by initiating a project to migrate virtual server subscribers to its AWS cloud tenant. VITA is currently architecting a robust multi-cloud connection strategy complete with applicable security controls for all other DR services. VITA anticipates reporting on the necessary associated investment next year.

CONCLUSION

The comprehensive initiatives undertaken to enhance network infrastructure and related security and services show the Commonwealth's commitment to modernized technological capabilities. These efforts are essential to meet the evolving demands of public service delivery while ensuring data security and disaster recovery readiness. By identifying and acting on areas of improvement, the Commonwealth is poised to advance its IT landscape and ensure efficient, secure, and reliable services to citizens and customer agencies.

Appendix A