VIRGINIA IT AGENCY

Commonwealth of Virginia

Enterprise Technology Architecture [ETA]

Wide Area Network [WAN]

vita.virginia.gov

February 15, 2023

Revision History

Network: Wide Area Network (WAN)		
Revision	Date	Description
1.0	01-01-2021	Initial
2.0	10-06-2022	The following new standards were added: • (Technology) WAN-53 – WAN-55 • (Bandwidth Allocation) WAN-81 – WAN-92 • (Availability/Performance) WAN-57 – WAN-80, WAN-93,95 • (Continuity) WAN-72 • (Security) WAN-94 The following existing standards were modified: • (Availability/Performance) WEB-20 • (Security) WAN-50 – WAN-51

Review Process

This standards document was posted on the Virginia Information Technologies Agency's (VITA) Online Review and Comment application (ORCA). All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were evaluated, and individual commenters were notified of action(s) taken.

Standards and Agency Exceptions

The standards included within this document are mandatory. Agencies deviating from these standards must request an exception for each desired deviation, and receive an approved *Enterprise Architecture Exception* via Archer, prior to developing, procuring, or deploying such technology, or not complying with a standard specified in this document. The instructions for completing and submitting an exception request are contained within the *Commonwealth Enterprise Architecture Policy*.

Glossary

As appropriate, terms and definitions used in this document can be found in the Commonwealth of Virginia Information Technology Resource Management (COV ITRM) Information Technology (IT) Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page on the VITA website at: https://www.vita.virginia.gov/it-governance/glossary/cov-itrm-glossary/.

Contents

Introduction

Vision & Strategy
Vision
The Commonwealth of Virginia Wide Area Network (COV WAN) will meet the business connectivity needs of our customer agencies. The WAN will be available and resilient. Root causes for WAN issues will be identified proactively before those issues adversely impact the business.
Strategy
Objective 1 All aspects of the WAN will have performance thresholds. Tools will be in place to measure, trend, report, and notify customers prior to any thresholds being exceeded. **Objective 2** Notifications for developing WAN performance issues will include root cause identification and recommendations for how to remediate those issues. **Objective 3** A software defined WAN (SD-WAN) will be implemented to increase the resiliency of the WAN. **Objective 4** Technology options beyond circuits will be available to customers when practical, to help them achieve their availability and resiliency needs.

Purpose

The purpose of this report is to provide technical standards for the commonwealth Wide Area Network (WAN).

A wide area network (WAN) is a network that exists over a geographical area. A WAN connects different smaller networks, including local area networks (LANs) and metro area networks (MANs). This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.

The Commonwealth enterprise technology architecture establishes an architecture model using seven primary viewpoints. Each viewpoint includes standards for how a technology architecture must be used to provide solutions. The viewpoint standards incorporate details about the purchase, design, implementation, and on-going operation of COV IT solutions and utilized technologies. The seven viewpoints include:

1. Technology
2. Design/Architecture
3. Availability/Performance
4. Capacity
5. Continuity
6. Integration/Interoperability [not applicable for this topic]
7. Security

Authority

Code of Virginia, §2.2-2007	Powers of the CIO
Code of Virginia, §2.2-2007.1	Additional duties of the CIO relating to information technology planning and budgeting
Code of Virginia, §2.2-2009(A)	Additional duties of the CIO relating to security of government information
Code of Virginia, §2.2-2012(A)	Additional powers and duties related to the procurement of information technology
Code of Virginia, §2.2-3818	Standards for authentication of electronic government records

Technology

These standards relate to optimization, return on investments, best practices, standard protocols, interoperability, and other specifications.

The intent is to identify efficiencies for technologies; increase compatibility, encourage use of industry best practices and reduce costs wherever possible.

WAN-01 COV shall migrate from the legacy wide-area network (WAN) to a software designed SD-WAN, all new Network WAN's shall include SD-WAN.

Note: SD-WAN with multi-path technology allows a business to simultaneously use wireless, cable broadband and a private IP service together to create a highly reliable, redundant network fabric that can dynamically adjust to almost any kind of outage.

WAN-02 The WAN transmission medium used to connect commonwealth sites shall include one of the following:

- Twisted Pair Cable
- Unshielded Twisted Pair
- Coaxial Cable
- Optical Fiber Cable
- 4G/5G Wireless Broadband

WAN-03 Network WAN service suppliers shall provide WAN acceleration tools that optimize traffic using compression and caching protocol optimization where sites on VITA's network have compatible application optimization Common Platform Enumeration (CPE).

WAN-04 Network WAN service suppliers shall provide implementable solutions to meet multiple agency security and application standards for remote access.

WAN-05 Network WAN service suppliers shall provide the capability for use of remote access services by third party vendors who provide data center support services via an Internet connection.

WAN-06 Network WAN service suppliers shall provide solutions that are access type independent.

WAN-53 Network WAN service suppliers shall identify network technology opportunities that enhance value for the COV annually.

WAN-54 Network WAN service suppliers shall recommend mitigation strategies for all circuits that are overutilized/saturated more than 70% during business hours.

Note: The recommendation strategy will need to identify outdated network hardware such as T-1 lines, defective devices, poor network design/configuration and how those issues will be addressed.

WAN-55 Network WAN service suppliers shall recommend high value WAN technologies that can be leveraged in current/future WAN optimizations throughout COV.

Note: WAN technologies to be considered include: 5G Ultra-Wideband, Virtual Private LAN Service (VPLS), Ethernet Virtual Private Line (EVPL), Multiprotocol Label Switching Network Virtual Private Network (MPLS VPN), Ethernet Private Line (EPL), Metro Ethernet, Internet Protocol Secure Virtual Private Network (IPsec VPN).

Bandwidth Allocation

Bandwidth is measured as the smallest capacity between the source and destination hosts. The intent is that sufficient bandwidth must exist to ensure the following allocations:

- 15% - Support for data transmissions supporting platform/system management
- 10% - Support for periodic bursts of network traffic
- 75% - Agency use

WAN-81 Network WAN service suppliers shall monitor, trend, and report local network bandwidth utilization.

WAN-33 Total agency site bandwidth shall be sized to support infrastructure management data transmissions that do not exceed an average of 15% during any day of the week.

WAN-82 Network WAN service suppliers shall notify COV when the data transmissions for infrastructure management have exceeded 15% during a business day.

WAN-83 Network WAN service suppliers shall deploy a tool that can isolate and identify what is causing the data transmissions for infrastructure management to exceed 15% during a business day.

WAN-34 Total agency site bandwidth availability shall be sized no less than 75% for agency business use during agency business hours.

WAN-84 Network WAN service suppliers shall notify COV when agency site bandwidth is less than 75% for agency business use over the business day.

WAN-85 Network WAN service suppliers shall deploy a tool that can identify when the total agency site bandwidth available for agency business use is less than 75% over the business day.

WAN-35 Total agency site bandwidth shall be sized so that non-business related usage does not exceed 10% during a business day.

WAN-86 Network WAN service suppliers shall notify COV when total agency site bandwidth for non-business related usage exceeds 10% during a business day.

WAN-87 Network WAN service suppliers shall deploy a tool that can identify and isolate what is causing the agency site bandwidth to exceed 10% for non-business usage during a business day.

WAN-36 The bandwidth utilized shall not exceed the specified bandwidth allocations for more than 2 hours per day.

WAN-88 Network WAN service suppliers shall notify COV when the bandwidth utilized exceeds specified bandwidth allocations for more than 2 hours per day.

WAN-89 Network WAN service suppliers shall deploy a tool that can identify when the agency site bandwidth exceeds specified bandwidth allocations for more than 2 hours per day.

WAN-37 Network WAN service supplier shall be able to report the total agency site bandwidth sized so that network traffic shall not exceed 90% of that bandwidth for over 2 hours per day.

WAN-90 Network WAN service suppliers shall notify COV when the total agency site bandwidth exceeds 90% of capacity for over 2 hours per day.

WAN-91 Network WAN service suppliers shall deploy a tool that can identify and isolate what is causing the agency site bandwidth to exceed 90% of capacity.

WAN-92 Network WAN service suppliers shall have recommendations on addressing all bandwidth issues.

Design/Architecture

These standards relate to overall architecture characteristics such as fault tolerance, durability, and scalability. They define and constrain while aligning to VITA standards and industry best practices. In ITIL, they relate to the areas of service design and service transition.

The intent is to create the services and experiences that VITA agencies and customers want and need through ensuring an effective design prior to implementation. Architecture and design should reflect the fair solution to a problem being resolved by ensuring the solution actually resolves the problem, and that a desired innovation adequately addresses various needs without undue disruption.

Validation occurs through sufficiently detailed design documentation showing appropriate traceability to stipulated standards, all VITA rules, standards, regulatory, and governance compliance, which includes such areas as training plans, metrics plans, testing plans, and deployment plans and validation must be approved through a formal architecture review process prior to implementation in the enterprise.

WAN-07 COV shall employ a hub-and-spoke WAN design.

WAN-08 All WAN central locations (hubs) shall be located within a Commonwealth centralized data center.

WAN-09 COV shall ensure that single points of failure do not exist at any hub within the network.

WAN-10 All connections providing access to systems sensitive to availability or integrity shall ensure single points of failure do not exist.

WAN-11 COV shall maintain one or more points of presence at COV's authorized data centers. No other locations shall maintain a point of presence.

WAN-12 Connections between COV and third-party locations shall be maintained only at COV's authorized data centers.

WAN-13 Network WAN service suppliers shall support Quality of Service (QoS) across the access networks. This includes: 802.1p prioritized Ethernet, MPLS-based access, Multilink Multiclass PPP, QoS-enabled wireless (LTE, wireless 802.11.x), cable high-speed access (DOCSIS 1.1), QoS-enabled Digital Subscriber Line (DSL), and QoS-enabled satellite broadband access.

WAN-14 End user agency traffic shall be routed based on assigned priorities, using different classes of service designations, which follow the Internet Engineering Task Force Differentiated Services or "Diff-Serv" model.

WAN-56 Network WAN services shall provide detailed quarterly reporting on routing efficacy and how it has improved performance.

WAN-15 Network WAN services shall provide a secure, end-to-end logical connection between resources on the managed WAN and transport services and agency remote sites connected to the Internet.

WAN-16 Private cellular wireless connections shall be provided as required to access specific MPLS VRF's through the private wireless gateway service.

WAN-17 Network WAN service suppliers shall provide the capability to use common broadband Internet services as a means to achieve private Wide Area Network (WAN) connectivity.

WAN-18 Network WAN service suppliers shall provide a method for agencies to utilize secure tunnels across the Internet to connect to the COV network.

WAN-19 Network WAN service suppliers shall provide the capability for public Internet access via a secure proxy service and prohibit "split tunnel" configurations that would allow users direct access to the public Internet (e.g., website, social networks, online gaming).

Availability/Performance

These standards relate to areas such as reliability, maintainability, and serviceability. In ITIL, they relate to the area of service design. Common areas of interest are service level agreements (SLAs), monitoring, tuning, analysis, testing, and reporting.

- Availability relates to any stop actions that are planned or unplanned. An unplanned action example is equipment failure. A planned action is system maintenance.
- Performance relates to a systems responsiveness to execute an action within a given time interval – it is a quality metric.

The intent is to ensure the stipulated solution and/or supplier is supporting or exceeding currently defined parameters in the enterprise.

Validation occurs through appropriate monitoring and reporting mechanisms. Common report type examples are System Availability, Response Time, API, Service Availability, and Number and Duration of Service Interruptions.

WEB-20 Physical WAN connections shall be designed so that:

- All WAN connections have an availability of 99.9% or higher
- All point of presence locations physical connections have an availability of 100%
- No single point of failure shall exist for any connection requiring an availability of greater than 99.9%

WAN-73 Network WAN service suppliers shall monitor, trend, and report latency for every circuit they support in COV.

WAN-21 Latency within the COV enterprise-wide area network and local area network (WAN/LAN) shall not exceed 100ms (roundtrip time of 200ms) between the source and the destination.

WAN-74 Network WAN service suppliers shall notify COV when latency exceeds 100ms (roundtrip time of 200ms) between the source and the destination for over one hour during a normal business day.

WAN-75 Network WAN service suppliers shall deploy a tool that can isolate the causes of latency.

Note: The tools and their usage need to be able to isolate causes of excessive latency (examples: under-performing hardware, interference from objects, distance between devices, misconfiguration and abysmal Internet connections, cabling)

WAN-76 Network WAN service suppliers shall make recommendations to COV on how to reduce latency based on their tool use.

WAN-77 Network WAN service suppliers shall monitor, trend, and report circuit capacity for every circuit they support in COV.

WAN-22 Circuit utilization must not exceed 90% of capacity for more than 1 hour over a business day.

WAN-78 Network WAN service suppliers shall notify COV when circuit utilization exceeds 90% for more than 1 hour over a business day.

WAN-79 Network WAN service suppliers shall deploy a tool that can isolate and identify what is causing the circuit to be overutilized/saturated.

WAN-80 Network WAN service suppliers shall make recommendations to COV on how to upgrade circuits that are overutilized/saturated based on their tool use.

WAN-24 Jitter shall be less than 30 milliseconds.

WAN-57 Network WAN service suppliers shall monitor, trend, and report jitter for every circuit they support in COV.

WAN-58 Network WAN service suppliers shall measure period jitter by measuring the duration of one clock period 10,000 times, and using the recorded data to calculate the mean, standard deviation and peak-to-peak values for every WAN circuit managed.

WAN-59 Network WAN service suppliers shall notify COV when jitter exceeds 30 milliseconds for over 20% of daily measures.

WAN-60 Network WAN service suppliers shall deploy a tool that can isolate the cause of jitter.

Note: The tools and their usage need to be able to isolate causes of excessive jitter (examples: under-performing hardware, interference from objects, distance between devices, misconfiguration and abysmal Internet connections, cabling)

WAN-61 Network WAN service suppliers shall make recommendations to COV on how to reduce jitter based on their tool use.

WAN-25 All proposed IT solutions that can impact the Wide Area Network (WAN) or the Local Area Network (LAN) shall ensure that Network Performance Simulation Modeling and Application Emulation (NPMAE) standards are included within the Request for Proposal (RFP).

WAN-26 IT solution providers shall perform simulation modeling to determine the impact on the WAN/LAN ability to support any additional bandwidth standards for any new IT solutions that will utilize the WAN/LAN.

WAN-27 IT solution providers shall perform emulation to assess the IT solution's impact on the current WAN/LAN network baseline and simulation model assumptions before the implementation of the application.

WAN-93 The results of the performance simulation and emulation shall be forwarded to VITA.

WAN-28 Network WAN service suppliers shall provide SONET or DWDM technology capable of fault tolerant, high bandwidth physical connectivity between campus buildings.

WAN-29 Network WAN service suppliers shall provide support for IPv4 and IPV6 as both the encapsulating and encapsulated protocols.

WAN-23 Packet errors and packet loss shall be less than 1%.

WAN-62 Network WAN service suppliers shall monitor, trend, and report packet loss for every circuit they support in COV.

WAN-63 Network WAN service suppliers shall monitor packet loss by measuring the number of packets not received divided by the total number of packets sent.

WAN-64 Network WAN service suppliers shall report packet loss when it exceeds 1% on a circuit for 1 hour or more during the business day.

WAN-65 Network WAN service suppliers shall deploy a tool that can identify the causes of packet loss.

Note: The tools shall need to be able to pinpoint the causes of packet loss by taking the following factors into account: network congestion, problems with the network hardware, software bugs, overloaded device, security threats, and faulty configuration changes.

WAN-66 Network WAN service suppliers shall make recommendations to COV on how to reduce packet loss.

WAN-95 COV shall have a process that can evaluate all technologies and suppler services that are available at any given agency location for best fit for meeting agency performance and availability standards. Agencies shall be provided a method for requesting that evaluation.

WAN-67 Network WAN service suppliers shall measure, monitor, trend, and report for every circuit they support within COV:

- Circuit capacity vs. Current circuit speed
- Recommended circuit bandwidth
- Device name and location
- Type of Circuit
- Report overutilized/saturated circuits above 70% capacity

WAN-68 Network WAN service suppliers shall be able to monitor circuit capacity in real time at multiple intervals with customizable indicators.

WAN-69 Network WAN supplier tools shall monitor and measure performance for all supplier provided circuits. The tools shall identify overutilized/saturated circuits and report as follows:

- 80 - 100%: Red
- 60 - 79%: Yellow
- 59% or lower: Green

WAN-70 Network WAN service suppliers shall utilize a tool that isolates the causes of network circuit saturation when requested by COV.

WAN-71 Network WAN service suppliers shall make recommendations to COV on how to reduce network circuit saturation.

Capacity

These standards relate to such capacity areas as upgrades, tuning, and monitoring. In Information Technology Infrastructure Library (ITIL), they relate to the area of service design. Capacity is concerned with meeting both current and future capacity, and the performance needs of the IT infrastructure.

The intent is to ensure IT services and infrastructure meet agreed upon standards in a cost effective and timely manner. The idea is to adapt to changing enterprise service levels through optimization and capacity increases that improve service levels while ensuring costs meet acceptable budget thresholds.

Validation occurs through applicable monitoring and reporting mechanisms such as capacity reports and workload analysis reports, updated Configuration Management Database (CMDB) information, and change approvals.

WAN-31 The combined bandwidth for circuits shall be a minimum of 100kbs (kilobytes per second) per network connected user at an agency location.

WAN-32 Each agency shall identify estimated bandwidth usage per application. The following must be maintained in Archer for each application:

- Number of average concurrent users on the application (concurrent is defined as users transmitting or receiving application data at the same time)
- Number of concurrent users during application peak usage time (i.e., visitors during tax season, hurricanes, document submissions)
- Estimated application bandwidth used
- The application throughput estimate (how much network traffic can be processed at once)

Continuity

- These standards relate to IT infrastructure components and resources (internal and external) such as facilities, equipment, systems, applications, data, and networks that are required to restore minimum acceptable service levels during an event, incident or disaster.
- **Note:** IT Information Security Standard (SEC501-12.0/CP-1-10) addresses the standards for the recovery of COV IT systems and data that support COV mission essential functions as determined in the agency’s Business Impact Analysis. Moreover, the Virginia Department of Emergency Management (VDEM) defines COV continuity planning standards.
- The intent is to support the rapid and orderly restoral of IT services due to such incidents as loss of facility access (building fire) and loss of service (equipment failure). In ITIL, they relate to the area of service design.
    - Validation occurs through such tasks as setting recovery point objectives (RPO) and recovery time objectives (RTO) and meeting those defined objectives in incidents, testing continuity plans, creating risk assessments, and creating risk reduction strategies.

WAN-38 Agency applications that are tracked in Archer as Sensitive to Availability or Integrity shall utilize an architecture that supports and provides sufficient continuity of application availability to support those business standards.

WAN-39 WAN standards for continuity must include support for high availability.

WAN-40 COV networks shall ensure that there is more than once connection medium between hubs and/or spokes.

WAN-41 Connection medium shall not have a single point of failure between source and destination.

WAN-42 All Point-of-Presence (PoP) connections originating from the hub shall maintain high availability at which two or more networks share a connection.

WAN-43 Agency locations that host applications sensitive to availability, and that utilize an alternate location to address that sensitivity, shall maintain high availability connections between the hosting sites.

WAN-44 WAN hubs shall maintain two different sources (2 pipes between centralized data centers).

WAN-45 Centralized data centers shall have multiple MPLS connections from two different carriers.

WAN-46 The different circuits that come into the centralized data centers shall enter the building at different locations.

WAN-72 COV WAN should use a multi-path approach with the use of technologies such as broadband wireless 5G, cable modem or satellite services to protect against outages.

Note: Multi-Path technology is designed to mitigate the effects of a host bus adapter (HBA) failure by providing an alternate data path between circuits.

Security

These standards relate to consistency of the security infrastructure across the enterprise in specific component areas such as monitoring, log collection, authentication, authorization, and patch management. As well as protection of enterprise IT assets, while managing risk to an acceptable/usable level. In ITIL, they relate to the area of service design.

The intent is to ensure authentication, authorization, and auditing be consistent across the enterprise, that patching, and upgrades are kept up-to-date, and that resources have acceptable levels of support provided by OEM’s and/or third parties.

Validation occurs through elimination of multiple sign-on administrations, decreasing risk factors, and specified reports.

WAN-47 COV assets, information, data and IT services shall meet business standards while maintaining confidentiality, integrity, and availability.

WAN-48 All point of presence locations shall utilize content filtering to allow or deny data transmitted from any hub or spoke.

WAN-94 Content filtering shall be able to evaluate all data permitted across the network to determine if it is permitted or not.

WAN-49 Network WAN service suppliers shall partition the remote access service such that it supports:

- Multiple agencies securely sharing the remote access service
- Multiple organizations and sub-organization relationships
- Agency-specified access control policies
- Policy enforcement of access authority

WAN-50 Network WAN service suppliers shall provide secure remote access via a secure channel Virtual Private Network (VPN), using strong cryptography and security protocols (e.g. Secure Sockets layer/Transport Layer Security (SSL/TLS), Internet Protocol Security (IPSec), Secure Shell (SSH)) to safeguard sensitive data during transmission over public Networks.

WAN-51 Network WAN service suppliers shall support multiple tunneling standards including Layer Two Tunneling Protocol (L2TP), Generic Routing Encapsulation (GRE), Encapsulating (or tunneling) the packets (IP-in-IP), Multiprotocol Label Switching (MPLS), Internet Protocol Security (IPSec), and Transport Layer Security (TLS).