



Modernize Public Sector Networks with Trusted SD-WAN

Thank you for downloading this VMware Case Study. Carahsoft is the distributor for VMware solutions available via GSA, NASA SEWP V, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring VMware’s solutions, please check out the following resources and information:



For additional resources:
carah.io/vmwareresources



For upcoming events:
carah.io/vmwareevents



For additional VMware solutions:
carah.io/vmware



For additional solutions:
carah.io/vmware



To set up a meeting:
vmware@carahsoft.com
888-6VMWARE



To purchase, check out the contract vehicles available for procurement:
carah.io/vmwarecontracts

For more information, contact Carahsoft or our reseller partners:
vmware@carahsoft.com | 888-6VMWARE

Modernize Public Sector Networks with Trusted SD-WAN



SD-WAN™

With FedRAMP High Authorization, VMware SD-WAN provides key benefits for the public sector

- Provide distributed workforces with secure and reliable access to cloud, no matter where they are—ensuring productivity to achieve mission objectives.
- Complement cloud-smart adoption with Trusted Internet Connections (TIC 3.0) to accelerate the journey towards zero trust.
- Gain long-term cost savings by supplementing existing MPLS connections with Direct Internet Access (DIA).
- Deploy SD-WAN rapidly at agency locations with cloud-delivered zero touch automated deployment, and centralized management with configuration, monitoring, and troubleshooting.

Government agencies are on a digital transformation journey

Across the public sector, agencies are laying the groundwork for cloud-smart adoption. 97% of agencies have a cloud strategy, with 37% of them actively using multiple clouds¹. Federal leaders are also looking at edge solutions² to realize the potential of specialized IoT devices such as cameras and sensors, and 5G services to connect them. As public cloud adoption and the number of applications continues to grow, so do the number of security threats.

Telework and remote work are becoming the new norm for many government agencies. In November 2021, the Office of Personnel Management (OPM) laid out a plan³ for reimagining how federal agencies work. The OPM recognized the many benefits of flexible workplaces, including the ability to continue critical government services during a disaster.

Legacy networks are a transformation barrier

Like the private sector, government workers need ubiquitous access to cloud applications and data. Agencies' progress towards accomplishing mission goals is hampered if this highly distributed workforce does not have adequate connectivity for fast and secure access to SaaS apps and cloud-based resources.

It is not uncommon to hear government employees complaining that network connectivity is faster at their house than at their office. Traditional network architectures for government agencies use a hub-and-spoke network to route traffic from agency locations through the headquarters, then back out to cloud-based applications and data sources, resulting in network bottlenecks and a poor user experience for the distributed workforce. This in turn affects

¹ [Issue Brief: Federal Cloud Infrastructure Survey Results Summary](#), Advanced Technology Academic Research Center

² [Federal edge solutions: Extending IT to the mission's edge](#), Accenture, September 13, 2021

³ [2021 Guide to Telework and Remote Work in the Federal Government](#), United States Office of Personnel Management, November 2021

employee productivity. Traditional networks are very expensive and difficult to scale to meet the performance requirements of cloud applications.

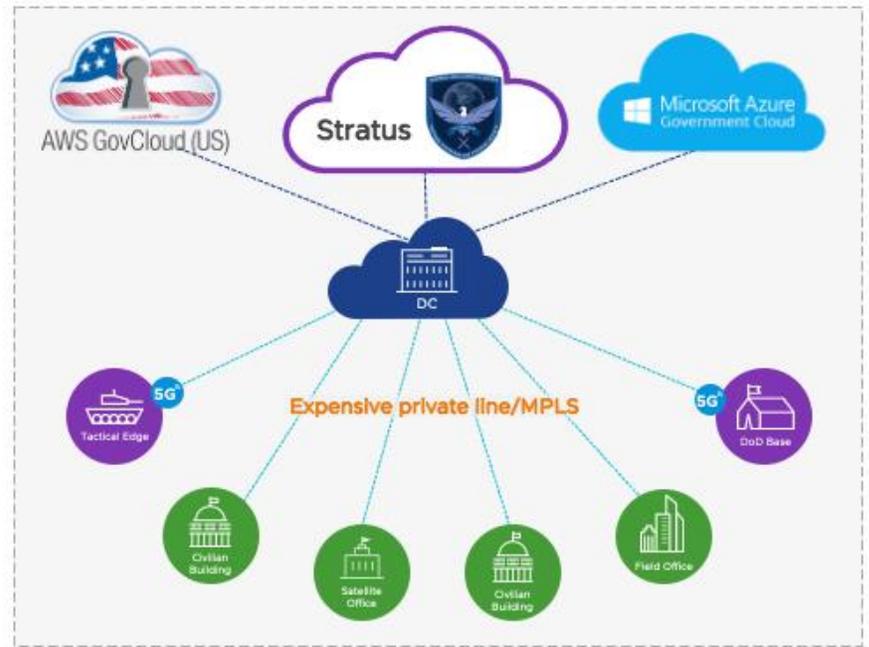


Figure 1: Legacy WAN cannot meet the evolving needs of the public sector

With the increasing use of public cloud and SaaS, applications accessed by government workforces are more distributed than ever across multiple geographic locations. This places even more pressure on WAN networks to deliver applications with service level guarantees and ensure an optimal user experience.

To address this growth in cloud adoption and successfully implement cloud-smart strategy, agencies need a software-defined WAN (SD-WAN) solution to provide optimal connectivity to multiple clouds.

Network modernization starts with VMware SD-WAN

VMware SD-WAN™ optimizes agency networks for multicloud, zero trust and the distributed workforce. It connects government employees across distributed agency locations securely, reliably, and efficiently to cloud-based applications, cloud services and agency data centers. Agencies can rely on VMware SD-WAN to improve employee productivity with secure and optimized application access, no matter where they are located.

VMware SD-WAN provides an application-aware solution that meets agencies' defined application service level agreements (SLAs) while delivering the best user experience for government workforces and ensuring productivity to

achieve mission objectives. VMware SD-WAN provides agencies the flexibility to use the connectivity of their choice (i.e., MPLS, broadband Internet, 4G/LTE, 5G, and SATCOM).



Figure 2: VMware SD-WAN connects government workforce securely, reliably, and efficiently to the cloud.

VMware SD-WAN: Built for government in the cloud

VMware is the only SD-WAN vendor today to achieve FedRAMP High Authorization⁴. Agencies don't need to settle for less anymore. FedRAMP High Authorization certifies that VMware SD-WAN can protect federal agencies' highly sensitive, unclassified information within a cloud environment. This allows government agencies to accelerate their path to the cloud.

VMware SD-WAN's cloud-first architecture for government follows the highly successful commercial offering with the added security and compliance requirements of federal agencies. With VMware SD-WAN, government agencies benefit from:

- **Optimized user experience:** Agency workforces get reliable and uninterrupted connectivity to cloud-based applications with Dynamic Multipath Optimization™ (DMPO). It can aggregate any available links, including broadband, 5G, LTE, satellite, and MPLS circuits.
- **Cloud agility:** VMware SD-WAN's cloud-first architecture for government complements the cloud-smart adoption. Agencies can leverage SD-WAN as a critical component of their multi-layered architecture while implementing initiatives such as Trusted Internet Connections (TIC 3.0) to help accelerate their journey towards zero-trust operations.
- **Simplified operations:** Agencies can rapidly deploy VMware SD-WAN at new or existing agency branch offices with cloud-delivered zero touch automated deployment. With stretched resources at smaller branches and satellite office

⁴ [FedRAMP Marketplace](#)

Learn more

- VMware SASE for government:
sase.vmware.com/solutions/federal-government
- VMware SASE: sase.vmware.com
- VMware SD-WAN:
sase.vmware.com/sd-wan

locations, agencies can manage the entire network from a centralized location.

- **Maximize ROI:** Agencies gain long-term cost savings by supplementing their existing MPLS connections with high-speed broadband or 5G/LTE services, and eliminating outdated, legacy hardware. VMware SASE customers can achieve an ROI of 218% with payback in less than 6 months.⁵

VMware SD-WAN is a simple, secure, and compliant solution for agencies modernizing their WAN networks. VMware SD-WAN is architected to reduce operational complexity while supporting the best user experience for cloud, SaaS, and legacy applications.

Government use cases

VMware SD-WAN's FedRAMP High Authorized solution supports use cases across Federal, SLED (State, Local and Education), Tribal government, and 16 critical infrastructure sectors. These use cases include:

- **Modernization:** Provide reliable, efficient, and secure connectivity between agency WAN sites and/or cloud applications. Complement or replace your MPLS connections with direct internet access (DIA) with your choice of broadband, 5G/LTE or SATCOM. DIA lowers network transport costs to agency networks and cloud services.
- **Zero trust:** Leverage VMware SD-WAN as a critical component of a multi-layered security strategy while implementing initiatives such as TIC 3.0 to help accelerate the journey towards zero-trust operations and meet Cybersecurity Executive Orders (EO).
- **Empower distributed teams:** Improve remote employee productivity and meet guidelines set by OPM. Highly distributed workloads and users require a software-defined WAN architectural approach for secure, agile, and optimal application access from agency branches, satellite offices or employees' homes.
- **Trusted Internet Connection (TIC) 3.0:** Provide guidance on delivering secure access to agency-sanctioned cloud services, web, and HQ to users in the agency branch office or working remotely for agencies that want to enable SD-WAN.
- **Tactical edge:** Improve communications to share critical DoD or national security information using SATCOM or 5G/LTE on the tactical edge, field offices or locations with no access to Ethernet connectivity.
- **5G/telco:** Leverage 5G/LTE as a primary or supplemental option for reliable and secure connectivity for agencies such as FEMA, law enforcement, and homeland security that need to set up field offices quickly.

⁵ [The Total Economic Impact™ Of VMware SASE: Cost Savings and Business Benefits Enabled By SASE](#), Forrester Research, February 2022