Transforming Government
with SD-WAN

The Government Agency's Guide to Network Transformation

Employing an edge-first SD-WAN strategy to meet agency network demands in the years ahead

HUGHES®
An EchoStar Company

@hughesconnects

government.hughes.com/sdwan

Better Security. Better Performance. Reduced Costs. SD-WAN is the Next Generation Agency Network.

Background

Government agencies face a daunting challenge: operating on legacy networks in an era of rapidly changing digital demands. In fact, 67% of federal IT professionals say their legacy network infrastructure struggles to keep pace with the changing demands of Cloud and hybrid technologies.[1] The same challenges plague IT professionals in the private sector, who cite security, complexity of transport types, need for better analytics, consistent performance of applications, and cost of bandwidth as areas of concern for distributed enterprise WAN solutions.[2]

Despite acknowledging the myriad issues with their legacy networks, federal IT professionals are falling behind with their agency modernization efforts. A recent GAO report found only 8 out of 19 federal agencies surveyed planned to be done with their transition to the GSA's Enterprise Infrastructure Solutions (EIS) contract by GSA's September 2022 milestone.[3] Agencies named complexity of the transition and insufficient IT personnel as the leading hurdles to a successful and timely transition to more highly performing networks.

Agencies wishing to modernize and meet the network demands of today and tomorrow, while staying within the boundaries of the federal procurement process, should find similar advantages as private distributed enterprise and implement Managed Software-Defined Wide Area Networks (SD-WAN). Already widely adopted and proven by commercial enterprises, Managed SD-WAN solutions offer federal agencies a clear path to network transformation that is proven today and future ready. Managed SD-WAN delivers Cloud readiness, robust branch security, and end-to-end optimization, with substantial performance improvements and cost savings over legacy networks. Federal agencies transitioning from the Networx contract to the EIS contract would be wise to take advantage of the availability of Managed SD-WAN solutions to improve current network operations and better prepare for future demands on their networks.

Different from an off-the-shelf SD-WAN solution, Managed SD-WAN is available only from a Managed Services Provider (MSP), like Hughes, that can tailor the SD-WAN solution to the agency's specific needs. In addition to equipment and broadband transport, Managed SD-WAN includes network operations, combined billing (often across providers), and security. Additionally, Managed SD-WAN comes with help desk support, typically available 24/7, based on service level agreements. Working with an MSP, the government agency receives the benefit of experience, proven implementation plans and professional SD-WAN management – freeing the agency IT team to focus on delivering value-added services to the employees and constituents.

This guide provides an overview of the challenges agencies face in transforming their networks to Managed SD-WAN, as well as proven strategies to overcome them.

1 MeriTalk's Cloud Complexity Study

2 https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/intelligent-wan/idc-tangible-benefits.pdf

3 https://www.gao.gov/assets/710/705755.pdf

Transition vs. True Transformation

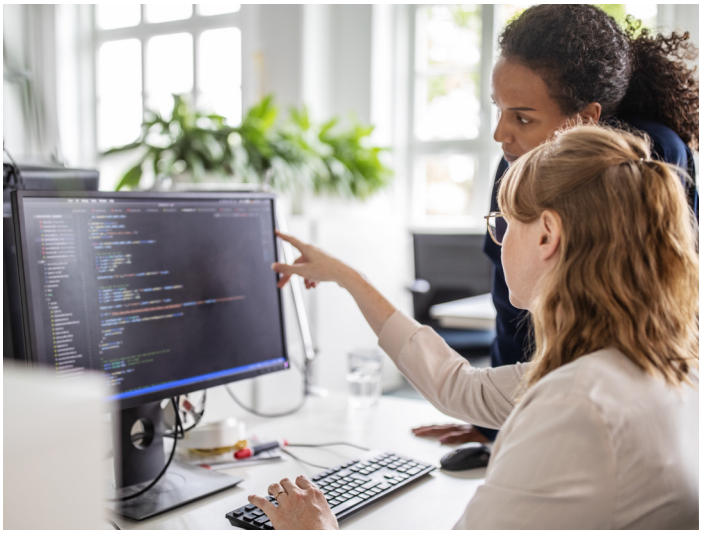
A Missed Opportunity Could be Costly

Even though the full transition deadline for EIS is not until 2023, do not accept a shortsighted, "like for like" approach. Doing so will create technology challenges in three primary areas – bandwidth, budget and security. Procurement cycles dictate that agencies need to act now and begin the process to modernize their networks. Most agencies operating on dedicated networks simply cannot afford to wait. If agencies do not seize the opportunity to modernize networks now, they face ongoing and mounting challenges.

1. Bandwidth Bottlenecks

Current federal agency networks cannot adequately support today's application demands, particularly at the field office. Cloud technologies, video streaming, teleconferencing, and other bandwidth-hungry applications are congesting traditional telecom infrastructure. And the demand for bandwidth will only continue to grow. Take, for example, the strain caused by the COVID-19 pandemic which forced agencies to implement wide-scale telework, not to mention the potential lasting implications of the trend toward remote work. The voracious appetite for bandwidth stretches far beyond unanticipated, temporary spikes.

Applications that once lived on the desktop now live on the Cloud or in a data center. In fact, Gartner predicts that through 2022, IT spending for cloud-based services and offerings will outpace non-cloud IT spending.[4] This is leading to increased bandwidth needs for organizations in both the public and private sectors. And in 2020, the COVID-19 pandemic has only increased the urgency for upgrading government agency networks – with several agencies considering strategies such as staggered work schedules to alleviate the strain on agency networks caused by mass telework. [5]



Imagine building the Mall of America on a two-lane country road without expanding the surrounding road infrastructure in anticipation of higher traffic. That's essentially what we're doing by expecting existing T1 lines to carry heavy cloud-based application traffic. Chasing more bandwidth on existing T1 lines is an expensive proposition – and the days of annual budget increases to cover those costs are over.

A like-for-like network transition all but guarantees the continuation of bandwidth constraints and budget shortages. Networks that already struggle to support field offices will find no relief if they do not transform now. The good news is, agencies do not need to scrap their existing MPLS networks to begin that transformation. By introducing managed broadband services with an intelligent, on-premise routing device, agencies can build upon what they have in place to create the more resilient, high-performing and cloud-ready networks of the future.

4 https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets

5 https://www.fedscoop.com/agency-bandwidth-maximum-telework/

2. Busted Budgets

Transformation to a smart network is more cost effective than transitioning existing technology. Agencies that adopt a like-for-like transition strategy assume the massive expense of continuing to maintain an all-MPLS network to dispersed field offices under a distance-sensitive pricing structure. The longer the line to reach a far-reaching field office, the more expensive the service and access costs. Bandwidth demand exceeding existing T1 capacity means adding more MPLS lines and quickly surpassing annual budgets.

Understanding that costs vary greatly by distance, agencies can expect to pay an average of $400-$600 per month per MPLS T1 line – which delivers a mere 1.5 Mbps download speed. That is not even enough bandwidth to stream a single, standard 1080p HD video – let alone effectively meet the data needs of conducting agency operations in 2020s.

Consider that the average cost of a broadband access line to that same location would fall somewhere between $100–$250 per month and likely deliver 25 Mbps to 100 Mbps download speeds per line. For agencies with hundreds or even thousands of locations, a truly modern network delivers huge benefit to budgets and efficiency. Further, the cost savings of broadband access justify the provisioning of diverse dual-path access for greater network availability and higher application assurance at the field office.

3. Security Concerns

While dedicated network technology, such as MPLS, delivers less bandwidth to field offices, it does come with a level of security that agencies find reassuring. In fact, some agency leaders believe that the introduction of broadband can expose their networks to hackers and cyber criminals who target government agencies daily. This has led some to hesitate on true transformation -- essentially sacrificing network and application performance for network security.

A distributed, broadband network does pose risks. A 2019 study by research firm Gartner titled "Invest Implications: 'The Future of Network Security Is in the Cloud'" finds that, today, "more users, devices, applications, services and data are located outside of an enterprise than inside."[6] Hackers often aim to exploit this to attack highly distributed organizations – Gartner estimates more than 30 percent of advanced threats target the distributed branch offices at the edge.

However, these risks can be mitigated with Managed SD-WAN. Agencies that implement Managed SD-WAN realize the cost and speed advantages of a broadband network plus the next-generation firewalls and ongoing monitoring necessary to greatly reduce – if not altogether eliminate – security risks.

6 https://www.gartner.com/en/documents/3957375/invest-implications-the-future-of-network-security-is-in

Modernizing Networks Through Managed SD-WAN

Transformation Now

For several years, commercial enterprises have been migrating to SD-WAN. In fact, according to a 2019 report from IDG Research, 90% of enterprises are actively researching, piloting, or using/upgrading SD-WAN for their organizations.[7] Benefits of SD-WAN include better network performance, improved security, increased bandwidth at a lower cost, flexibility (including more options for connection) and scalability. These benefits are not limited to the commercial enterprise. Federal agencies that implement SD-WAN now will yield similar benefits and be well positioned to adapt seamlessly to rapidly changing network demands. More than just lower costs, the commercial enterprise and the federal agency both are better equipped to serve the constituent, guest, customer or patron. The added speed and bandwidth enable modern, cloud-based applications, which make for a better constituent and employee experience.

It saves time and effort at the outset.

The Value of an MSP & How to Get Started with One

Early commercial adopters of SD-WAN found that a proven Managed Services Provider (MSP) can support or automate many of the complex planning stages, management and optimization processes amid an evolving security landscape.[8] In fact, a 2019 survey conducted by IDC found that "secure connectivity to cloud apps, the ability to improve performance of these cloud apps and the ability to automate and simplify management of WAN infrastructure" were chief drivers of SD-WAN adoption in the enterprise.

These same benefits are available to federal agencies. For instance, by executing network transformation to SD-WAN via an MSP, agencies can access multiple broadband services to most of their locations. This is critical for two reasons. One, because it gives agencies the opportunity to select best-of-breed broadband at each individual location. And two, because, if a site has an existing MPLS connection with a broadband access overlay, the MSP can use intelligent routers to prioritize application traffic based on automated policy rules programmed within each branch device. What's more, agencies already under pressure to meet network transformation deadlines and expectations are better off outsourcing this time and resource-intensive effort to an MSP rather than trying to replicate these capabilities in-house.

7 https://files.masergy.com/hubfs/White%20Papers/2019%20SD-WAN%20Market%20Trends%20Survey%20Data%20-%20IDG.pdf

8 https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/intelligent-wan/idc-tangible-benefits.pdf

Another way to streamline the transformation process is to issue a "statement of objectives" instead of a traditional "statement of work" to find the most cost-effective provider. With a statement of objectives, an agency gathers location-by-location service level agreements (SLAs) and lists them in a simple document, rather than having to map out and design an entire modernized network under a statement of work. With a site-specific statement of objectives, the MSP's network engineering experts can bring forth creative, efficient and lower-cost solutions for the agency to pursue the best architecture for the network they need. It saves time and effort at the outset.

Step-Wise: Start at the Edge with Hybrid Networking

Network transformation can be daunting, so a good place to start is where the impact will be most dramatic. For government agencies, the biggest opportunity for network transformation exists at the network's edge, where the agency interacts with the citizen and fulfills its mission. With limited budgets and resources, agencies will see the greatest impact from the transformation process at the edge.

An edge-first transformation plan provides an outside-in approach that can be executed faster and more easily, with minimal operational interruption – especially when implemented as part of a managed service. By delivering managed broadband services to field offices and automating network traffic using an advanced SD-WAN router, field offices get the secured bandwidth they need from multiple paths of connectivity. Creating a hybrid architecture – by adding managed broadband services to existing MPLS networks – effectively transforms and modernizes agency endpoints in relatively short order.

It's important to note that transition under this edge-first, hybrid approach does not impact the core of an agency's network where most of the existing technology is adequate. Strategically, this approach saves the core to be the last piece of the network to transform, enabling a well-calculated and least-disruptive evolution.

Prioritize Security

For agencies transforming their networks, accounting for robust security is paramount. When adopting an SD-WAN solution, do not assume it includes appropriate security. In fact, research from Fortinet, whose industry leading firewall technology is integrated with Hughes routers, indicates that 90 percent of SD-WAN solutions employ only basic security with a stateful firewall that merely allows or denies traffic. On the other hand, an SD-WAN solution can (and should) include firewall protection as well as intrusion prevention and detection built into the edge device. This is known as a next-generation firewall (NGFW) and its advantage is in the ability to inspect traffic to identify threats or threat patterns. This kind of edge-based approach to SD-WAN security mitigates risk and maximizes the benefits of a cloud-based enterprise network without depending on another piece of hardware to protect the local site and enable cloud connections. This is especially crucial amid rampant phishing and ransomware attacks that can wreak havoc on webservers, laptops and mobile devices.

Failure within any single agency site or application has the potential to result in a major outage. Because edge security is enforced locally at various points in the network, that risk is mitigated. Placing security closest to where the vulnerabilities lie also allows for scrubbing traffic that is wholly local to the site or travels site-to-Internet. This kind of traffic can include anything from office applications such as Office365 and Google Mail to government-specific applications for GIS data and video image recognition. With the ability to scrub this data – keeping bad data out while securing sensitive data before it leaves – edge-based security creates an inherently distributed security model, removing the risk of a significant breach resulting from a single point of failure.

The Benefits of SD-WAN are Proven

Support the Latest Applications

Government agencies interested in the benefits of SD-WAN can look to the private sector for proof of the benefits. Retailers and other multi-site enterprises have benefitted for years from tools like big data analytics, video training and cloud storage. These enterprises overwhelmingly are turning to SD-WAN to support those, and other, modern cloud based applications to improve operations. By increasing network availability and application assurance all the way from the edge to the cloud, network transformation that includes SD-WAN enables government agencies to take full advantage of these kinds of applications to achieve their missions.

Agencies without a purpose-built network to support critical operational functions at every location risk under-utilizing emerging cloud services, or worse, not being able to deploy them at all, resulting in additional wasted resources.

Network transformation is a process: it is not an event.

Commit to the Process

Network transformation is a process; it is not an event. The hybrid network architecture at the edge makes for an ideal phased approach for agencies, leveraging both broadband and existing MPLS transport technologies.

Rather than replacing one network for another, the most effective transformations build upon existing infrastructure as a foundation. For example, enhancing the existing MPLS network with the addition of secure, managed broadband lines and intelligent software-based orchestration of automated multi-path networking. This approach, which can be fully managed 24/7 by a proven, trusted provider, delivers high application availability – ending frustrations with application buffering or choppy VoIP calls. It also assures the agency of accountability and coordination across the network, regardless of how many or how widespread the locations, with a single source for network operation center (NOC) and security operation center (SOC) services. Moreover, by centralizing contracts from a patchwork of local service providers, a single MSP frees the agency's network team from juggling dozens of agreements across multiple carriers with different terms, conditions, and support channels.

The roadmap to network transformation starts now and at the edge with Managed SD-WAN solutions that can grow and evolve to meet the agency's network demands.

Appendix: Technical Specifications for Managed SD-WAN Solutions

Below are common technical tasks and services considered for a high-quality Managed SD-WAN solution.

- WAN optimization technologies
- Application classification and prioritization
- QoS and flow control
- Dynamic path selection
- Application-agnostic TCP acceleration for higher latency links
- Data compression for emails, office files, and unencrypted workloads
- Caching for repetitive downloading of common files and assets

VPN Support

- IPSec, AES encryption
- Networking/routing configuration
- Multiple WAN link support, DHCP, policy-based routing, RIP, OSPF, BGP, and multicast
- IPv4 support for operations and security components. (e.g., firewall, DNS, transport mode, SIP, dynamic routing)

Network Engineering Design Services, Implementation, Management, and Maintenance

- Provisioning, managing, and maintaining all end-point premises equipment and service-enabling equipment
- 24/7 network and security operations support and monitoring
- Management and monitoring of firewalls, including content filtering, Intrusion Detection and Prevention Systems (IDS/PS), and antimalware protection
- Integration with the agency's service desk, if applicable
- Engineering support and coordination for the provisioning of services
- Timely and accurate response to agency requests for status, information, performance, and service-level compliance reports
- Troubleshooting tools and analytics reporting for all broadband access technologies (including DSL, cable, fiber, Ethernet, 3G-4G, LTE wireless, microwave, and satellite)
- Field maintenance and troubleshooting of service issues
- Scalable bandwidth (high-capacity access) in increments up to 155 Mbps to agency field offices; multiple broadband links may be used to accommodate required bandwidth
- Provide full network capacity insights
- Real-time monitoring of links with dynamic balancing for better performance
- Multi-tier Help Desk support

More About Hughes

Hughes, known for its world-leading satellite network technology, applies its deep expertise in optimizing large and complex networks to include terrestrial network technologies to overcome obstacles faced by enterprises and government agencies. Hughes delivers managed wireline, wireless, and satellite broadband services to hundreds of commercial and government customers and has done so for over 15 years. Its approach is anchored by vast supply chain relationships with national and regional service providers that span the range of broadband technologies, such as cable, fiber, DSL, microwave, wireless (4G LTE), and its own market-leading High Throughput Satellite service. Hughes partners with multiple primes to serve the federal sector. The company's HughesON™ managed network services provide complete connectivity solutions employing an optimized mix of satellite and terrestrial technologies and have already resulted in agencies achieving twice the bandwidth at prices between one-third to one-half the cost of dedicated service lines to field offices.

Headquartered outside Washington, D.C., in Germantown, Maryland, USA, Hughes operates sales and support offices worldwide, and is a wholly owned subsidiary of EchoStar Corporation.

Meet the Network for the Era of More

More applications. More devices. More demands on government. For federal agencies, this is the Era of More. Fortunately, there's a network ready to support more. More bandwidth. More cost savings. A more responsive government, at every site and every location.

HughesON™ SD-WAN. The government's network for the Era of More.

HUGHES®
An EchoStar Company

Learn more at government.hughes.com/sdwan