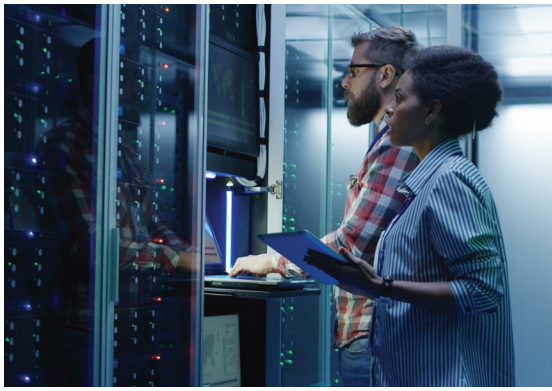
Transforming Government with SD-WAN

Federal agencies are beginning to transition from the General Services Administration (GSA) Networx contracts to the new GSA Enterprise Infrastructure Solutions (EIS) contract, a 15-year, $50 billion contract that will serve as the government's primary vehicle for procuring telecommunications-related services.



The new contract will usher in a new era of digital transformation that will help government agencies overcome a growing challenge: operating on legacy networks with ever-evolving application demands. It comes as no surprise that two thirds (67%) of Federal IT professionals say their legacy network infrastructure is struggling to keep pace with the changing demands of cloud and hybrid technologies.[1] What's more? Despite the perception of strong security elements in legacy systems, failing to transform will leave our agencies vulnerable to cyber threats at the edge. An overwhelming 86% of DoD managers say failing to modernize legacy DoD systems is putting the security of our nation in jeopardy.[2]

The problem? Fifty-one percent say their agency is failing to prioritize the networking aspect of cloud adoption and overall IT modernization.[1]

So, what's the solution? Agency network teams are increasingly turning to Software Defined Wide Area Networks (SD-WAN) that optimize and secure affordable broadband connections into cloud-ready enterprise-grade networks. Already widely adopted across the private sector, *managed* SD-WAN solutions offer agencies the best guidance for customized network transformation by leveraging the expertise of a proven Managed Service Provider (MSP). Benefits include cloud readiness, robust branch security, and end-to-end optimization, with substantial performance improvements and cost savings over legacy services. Additionally, managed SD-WAN solutions keep security prioritized by including 24x7 monitoring, threat protection, intrusion prevention, web filtering, and application control.

What are agencies' biggest network transformation challenges, and how can they realize success with SD-WAN?

The Network of Yesterday…and Today

With the first significant EIS transition milestone now in the rear-view mirror, some agencies are finding they underestimated the time required to prepare network modernization and transformation plans. The problem is compounded for large distributed agencies with hundreds or thousands of locations – the larger the network, the more complex it is to connect, manage and secure all the agency field offices. As a result, the temptation for agencies is to consider short-term "like-for-like" transitions over full-fledged modernization. This would be a lost opportunity, keeping the expensive decades' old network technology in place despite it not being adequate to support cloud, and other bandwidth-intensive applications.

New cloud-based apps demand more bandwidth and adding more bandwidth is too expensive in a distance-sensitive cost structure for legacy technologies like Multiprotocol Label Switching (MPLS) T-1 lines. At a roundtable discussion in 2018, a C-level government IT thought leader emphasized network concerns admitting, "Everything we want to do right now is going to require a significant amount of bandwidth, outside our normal datacenter-to-datacenter sort of bandwidth."[3]

How can agencies overcome legacy network challenges?

The Emerging Landscape for Federal SD-WAN Adoption

While still in the early stages of adoption, 29% of civilian agency IT professionals say they are working to lay the foundation for more modern networks.[1] Almost a third (32%) of DoD agency IT managers say they've increased virtual networking and/or Software-Defined Networking (SDN) over the past two years.[1] The new Trusted Internet Connections (TIC 3.0) policy, released by Office of Management and Budget (OMB) on Sept. 12, 2019, includes use cases for SD-WAN technology at agency branch offices.[4]

Rather than scrapping existing MPLS networks, agencies can build upon them to create more resilient, high performing, and cloud-ready networks. This is where SD-WAN comes in. SD-WAN solutions are designed to support on-premise traffic, public or private clouds, and Software as a Service (SaaS) applications unlike a traditional WAN which is router-centric and lacks the intelligence for reliable cloud application performance. SD-WAN further supports modernization efforts by using next generation firewall technology to securely connect to cloud resources, even in hybrid and multi-cloud environments. "Secure" SD-WAN solutions are the most performance and bandwidth friendly since they eliminate unauthorized or malicious traffic before any SD-WAN computation is executed.

Some Federal IT decision makers have expressed concerns with using broadband transport technologies like cable, fiber and 4G LTE, believing it opens their networks to cyber threats. However, managed SD-WAN solutions leverage an edge-centric security strategy to mitigate these risks. This approach intelligently secures each network endpoint – no matter the size of an agency's distributed network or devices that are connected locally. With a managed SD-WAN, agencies can benefit from end-to-end encryption across the entire network, including over the internet, so that all network endpoints are authenticated. Additionally, when SD-WAN is implemented as-a-service, agencies can rely on their proven Managed Service Provider (MSP) to monitor their network 24 hours a day, 7 days a week.

The Path Forward

Federal initiatives – such as TIC and migration to GSA's EIS contract – show the government's increased appetite for network transformation. And while the public sector has struggled to modernize legacy systems in a timely manner and without disrupting the agency mission, flagship examples already exist in government that promise a significant step forward. Failing to transform out of fear of security levels around new technology is natural. However, if agencies are paralyzed by that fear, then modernization will never take root. Just less than a decade ago, there was a similar fear around a new technology when cloud services rose to prominence. Many government organizations resisted the technology due to fears around the security of data being stored outside of their premises. Then, in 2014, the Central Intelligence Agency awarded a $600 million contract to AWS, which proved that, while the fears were understandable, there was a path to modernization when done in a calculated manner.

In early 2019, National Aeronautics and Space Administration (NASA) took the leap toward SD-WAN adoption when awarding the first task order under GSA's EIS program. The Department of Justice (DOJ) followed suit when awarding a 15-year contract for SD-WAN solutions and other network modernization efforts.[5]

And moving forward, the biggest opportunity for network transformation for government agencies exists at the network edge, where the agency meets the citizen and the mission is largely fulfilled. Agencies with large distributed networks and limited internal resources for conducting transformation in-house will find the most significant impact at the edge by deploying SD-WAN as a turnkey managed service.

An edge-first transformation plan provides an outside-in approach that allows agencies to get started today and with the sites that need bandwidth relief the most. When implemented as part of a managed service, IT leadership can achieve success faster and with minimal to no impact on operations. By delivering managed broadband services to field offices and automating application traffic using an intelligent SD-WAN on premise device, field offices can 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.

Fortinet + Hughes Network Solutions = Security & Performance

Fortinet's Secure SD-WAN solution uses a software-based service that runs on a single platform and includes routing, critical network functions and applications, and comprehensive network security – all of which seamlessly integrates into complex distributed networks. Fortinet's FortiGate Secure SD-WAN solution includes next-generation firewall (NGFW) security, advanced routing, and WAN optimization capabilities to deliver a security-driven modern networking solution. With a technologically advanced MSP partner in Hughes, Fortinet's largest MSP partner, this package of security and WAN optimization delivers the full potential of SD-WAN. Fortinet and Hughes bring expertise and execution to the same plane.

Together, Fortinet and Hughes bring you a wealth of experience in SD-WAN engineering and migration. The two companies have a strong hold on the market and a proven solution set – the relationship spans 12 years and includes more than 50,000 units deployed and managed for customers to ensure the security and performance of their networks.

The roadmap to network transformation starts at the edge, with managed SD-WAN solutions that grow and evolve to meet the agency's network demands – now and into the future.

For more information, please visit:
fortinet.com/products/sd-wan/ and government.hughes.com/sd-wan

FORTINET | HUGHES

[1] https://www.meritalk.com/study/sd-wan-the-next-federal-network/
[2] https://www.meritalk.com/study/innovation-imperative/
[3] https://government.hughes.com/collateral-library/government-agency-guide-to-network-transformation
[4] https://www.meritalk.com/articles/tic-3-0-draft-removes-barriers-for-emerging-technology/
[5] https://www.fiercetelecom.com/telecom/at-t-reels-984-million-contract-department-justice