MeriTalk

Underwritten by:

RUCKUS
COMMSCOPE

DELL
Technologies

The Future of Connectivity: Federal Network Modernization

Federal government networks are under more pressure than ever before. The number and diversity of connected devices and systems, and the data they generate, are exploding. The rise of edge computing and the Internet of Things is extending networks even further and enabling yet more data collection and transmission. As emerging technologies – from artificial intelligence (AI) and machine learning (ML) to 5G – grow more available, data transmission requirements and network complexity increase exponentially.

Although the Federal government spends more than $100 billion on IT and cyber-related investments each year, experts say Federal networks continue to require urgent modernization to meet mission requirements. The U.S. Government Accountability Office (GAO) has a long history of documenting legacy networks and other systems that introduce critical risks over time.

"A lot of Federal networks, unfortunately, have been neglected," said Duke Butler, vice president for business development at RUCKUS, a network solutions provider. "They haven't had aggressive upgrades, or in some cases, necessary maintenance. They have legacy components that restrict performance and open up security holes."

A recent MeriTalk study, conducted in partnership with RUCKUS and Dell Technologies, confirmed those concerns. Ninety-five percent of the 150 Federal government telecommunications decision-makers surveyed in November 2023 said they are experiencing frustrations with their current network, and 82 percent of agencies said their network impedes their ability to meet evolving mission demands. **Eighty-five percent** said that **now is the time for network modernization**.

"Connectivity demands continue to escalate," said James Wynia, director of product management networking for the Enterprise Solutions Group at Dell Technologies. "Meeting those needs is critically important."

This paper will share in-depth results from the MeriTalk study, show how modernization is progressing, outline modernization benefits, and demonstrate the value of a multivendor network strategy.

Today’s Networks Face Relentless Demands

The government today operates at mission speed – or it aspires to do so. Agency personnel need the right information, delivered at the right time, securely. Growing cybersecurity threats and sprawling networks make realizing this goal increasingly complicated – but not elusive.

The staggering number of network-connected devices and the vast amounts of data they generate are taxing outdated network infrastructures daily. The MeriTalk survey revealed that 44 percent of respondents say their network hosts at least 1,001 and as many as 5,000 devices.

How many devices are currently on your network?

Less than 500	21%
500 to 1,000	25%
1,001 to 5,000	44%
5,001 to 10,000	9%
More than 10,000	1%

Agencies know the demand for connected devices and data will continue to challenge their network capabilities. While some newer networks are mission assets, many others are outdated, impacting speed and reliability, which is especially problematic as data volumes increase. For data centers and large data processing or research functions that use large data sets or host sensitive data, outdated networks contribute to security issues and difficulty enabling AI and ML.

To fulfill their missions, agencies realize they must keep pace with relentless demand by investing in innovative networking technologies that are scalable, agile, and secure. They recognize the immediate and ongoing need for network transformation to achieve greater efficiencies and better performance and reduce costs.

> “By adopting a modern network, we can effectively reduce our agency’s IT costs through task automation, infrastructure consolidation, and optimization of bandwidth usage.”
>
> *– Federal government telecommunications decision-maker*

Network Modernization Is a Growing Priority

Awareness of the growing need for network modernization extends from within agencies to the top levels of government, where leaders across administrations have focused on it. Two executive orders (EO) in particular, on cybersecurity and customer experience, made IT modernization a government-wide priority.

The cybersecurity EO, issued in May 2021 after cybersecurity incidents such as SolarWinds and Colonial Pipeline, includes mandates on modernizing cybersecurity defenses and moving the government to secure cloud services and zero trust security architectures.

The customer experience EO later that year placed modernization in the context of enhancing government service delivery, instructing agency heads to “improve the digital customer experience for their respective agencies’ customers by modernizing agency websites, using human-centered design methodologies, digitizing agency services and forms, modernizing records management, (and) updating network infrastructure and mobility capabilities.”

In 2023, the National Cybersecurity Strategy heightened the focus on network modernization, saying cybersecurity goals “cannot be achieved unless Federal IT and OT systems are modernized so they are capable of leveraging critical security technologies.”

The COVID-19 pandemic also forced rapid network modernization in government by accelerating the shift to telework and digital service delivery, a result that can be seen in the proliferation of devices revealed in the MeriTalk survey.

Data Growth Drives Network Modernization

The MeriTalk survey revealed both the urgency of network modernization and optimism for it. Top drivers for modernization include data growth at the edge (cited by 37 percent of respondents), followed by cloud integration (33 percent), and quality of service (33 percent). About one in four (23%) said data at the edge is growing faster than they can handle.

Eighty-four percent believe a modern, agile network is crucial to their agency's ability to efficiently adapt to changing mission requirements and technologies, and almost half (45%) feel strongly that a modern network would improve their agency's cybersecurity posture and resilience. Recent cyberattacks targeting Federal agencies, such as the breach of MOVEit data transfer software in June 2023 and the July 2023 breach of Microsoft webmail, underscore the network modernization-cybersecurity priority.

What is driving your agency's focus on network modernization?

- #1 Data growth at the edge **(37%)**
- #2 Cloud integration **(33%)**
- #2 Quality of service **(33%)**
- #4 Scalability requirements **(32%)**
- #4 Increased data traffic **(32%)**

Network Modernization Needs to Accelerate

Despite the growing importance of network modernization, government reports and survey results show that the pace of change needs to quicken. A recent GAO report observes that the Federal government has long "had difficulties acquiring, developing, and managing IT investments," while also struggling with "appropriately planning and budgeting for modernizing legacy systems; upgrading underlying infrastructure; and investing in high quality, lower cost service delivery technology."

In the report, GAO laid out the consequences of failing to update legacy systems, including security risks, unmet mission needs, and increased costs. While some progress has been made in network modernization, the watchdog agency noted, more work is needed – especially at Federal agencies that have not developed complete modernization plans.

GAO's conclusions mirror the results of the MeriTalk survey, which found that network modernization has significant room for growth. Forty-one percent of respondents feel strongly that their current network impedes their ability to meet evolving mission demands.

That's because of a series of challenges with current networks identified in the MeriTalk research. Top challenges include:

#1
Scalability limitations
(32%)

#2
Security concerns
(30%)

#2
Difficulty deploying new applications
(30%)

#4
Difficulty integrating emerging technology
(29%)

Going forward, 50 percent of respondents said network modernization is their No. 1 IT priority, while an additional 45 percent called it a top priority. At a time when senior government officials are saying that America is engaged in a cyber war amid rising attacks on U.S. infrastructure and growing cyber capabilities of foreign adversaries, the modernization imperative could not be more clear.

In addition to cybersecurity improvements, modernizing to replace legacy systems with more efficient, high-bandwidth networks based on open standards will "support modern workloads, offer seamless connectivity, and improve performance and reliability," noted Saurabh Kapoor, director of product management and strategy for emerging networking technologies at Dell Technologies.

For Wynia, of Dell Technologies, that modernization means purpose-driven networks, those that combine "the best technology available – such as cloud-scale networking capabilities, edge, and next-generation switching – to meet specific agency objectives. These networks are scalable and customizable."

Open-source solutions including Software for Open Networking in the Cloud, or SONiC, a Linux-based network operating system (NOS), are helping agencies accelerate adoption of modern network architectures, experts say. SONiC runs on switches from multiple vendors, providing agencies with the flexibility of a single NOS in a multivendor ecosystem. The result is increased agility, resiliency, and scalability.

The Enterprise SONiC Distribution by Dell Technologies, for example, offers the benefits of SONiC with enterprise support and feature additions to extend its capabilities from the edge to the core to the cloud.

New Technology Can Help Accomplish the Mission

The next generation of technology, experts say, is needed to effectively modernize Federal networks. The MeriTalk survey shows that it is rapidly emerging – and, in some instances, is already here.

Federal telecommunications leaders said a variety of network modernization efforts are in progress, led by AI solutions and 5G network integration (each is currently underway with 51 percent of respondents). Half of respondents said their agency has begun to implement AI at the edge, with an additional 32 percent planning to start deployment in the next two years. Overall, agencies see 5G and AI as having the most significant roles in their network modernization roadmaps over the next five years.

Also high on the list of current modernization initiatives are network automation and/or optimization (48 percent); network virtualization or software-defined networks (46 percent); Internet of Things network expansion (43 percent); single pane of glass solution for network monitoring (41 percent), and multicloud management (39 percent).

Where does your agency stand with each of the following network modernization efforts?

	In progress	Short-term goal (within next 2 years)	Long-term goal (beyond 2 years)
5G network integration	51%	25%	19%
AI solutions	51%	29%	14%
Network automation and/or optimization	48%	35%	11%
Network virtualization or Software-defined networking (SDN)	46%	39%	12%
Internet of Things (IoT) network expansion	43%	33%	17%
Single pane of glass solution for network monitoring and analytics	41%	34%	17%
Multicloud management	39%	37%	14%

Also expected to play a major role is Wi-Fi 7, considered to be the next generation in Wi-Fi technology with its extreme speeds, low latency, and increased capacity. Wi-Fi 7 will be core to driving value from AI, ML, and edge computing investments and providing a more efficient, secure, and responsive network overall, experts say. Ninety-nine percent of survey respondents said they expect benefits from Wi-Fi 7, including:

Enhanced quality of service	39%
Increased signal quality	34%
More reliable connectivity	34%

Three in ten respondents expect to incorporate Wi-Fi 7 into their agency's network within the next year, and an additional four in 10 foresee Wi-Fi 7 incorporation within the next three years.

While **43 percent** of survey respondents feel strongly that **Wi-Fi 7 will revolutionize government connectivity**, agencies with multivendor networks are significantly more likely to feel that way compared to agencies using a single-vendor approach (52 percent vs. 34 percent).

> “Wi-Fi 7, along with the new 6 GHz band, offers an unprecedented opportunity to increase network performance.”
>
> *– Siân Morgan, Research Director, Dell'Oro Group*

A Multivendor Approach to Network Modernization Offers Myriad Benefits

The differing views on Wi-Fi 7's potential highlight what experts say is an important issue in network modernization and operation. A multivendor approach, they say, is more effective than a single-vendor strategy in providing security and achieving high performance and other key metrics.

“Many organizations will settle for a single vendor that can check the most boxes. Historically, this solution provides the most mediocre outcome,” said Butler, of RUCKUS. “Multivendor solutions that provide best-of-breed functions, performance, and ability to respond to changing parameters enable the best outcomes.”

Kapoor, of Dell Technologies, added that a single-vendor approach can limit innovation.

"Dependency on a single vendor makes the government heavily reliant on specific technologies, products, and solutions provided by that vendor," he said. "That limits the flexibility to switch to an alternative solution that is more advanced."

As agencies continue to transform and modernize their networks, a multivendor network strategy encourages innovation and increases competition to reduce costs. Government leaders know that competition is the driving force behind innovation and value.

Concerns about a single vendor approach are reflected in the MeriTalk survey. Though the survey found that agencies today are evenly divided between using a multivendor and a single-vendor approach for their primary network infrastructure, respondents from multivendor agencies expressed concern that a single-vendor system limits flexibility and competitive pricing. Agencies with a single-vendor network strategy said that limited innovation is their top concern with using a single vendor.

Perhaps most importantly, given the urgency of modernizing Federal networks with new technologies, single-vendor agencies were significantly more likely than multivendor agencies (36 percent vs. 21 percent) to have difficulty integrating emerging technology.

Agencies Should Accelerate Modernization – Now

The benefits of transforming and modernizing Federal networks are significant – speed, reliability, redundancy, and security top the list. Modern networks are designed to deliver these benefits and are purpose-built to meet specific agency requirements. They are critical to delivering citizen services, supporting our nation's warfighters, and defending against evolving threats. They are essential to increasing efficiency and reducing costs.

Federal government telecommunications decision-makers say a multivendor network strategy:

"allows us to select best-of-breed solutions for specific network needs"

"encourages innovation, healthy competition, and pushing the limits of AI applications"

"can improve service reliability by avoiding single points of failure"

"[provides] potential cost savings through competitive pricing and negotiation power"

The risks associated with the status quo are far greater than the costs of modernizing. To accelerate modernization, agency leaders will need to aggressively drive change by:

- Pursuing a strategic, multivendor strategy to ensure flexibility, scalability, innovation, and competition to achieve the best value and optimal performance
- Enforcing the use of open standards to accommodate best-of-breed, multivendor network solutions
- Linking network acquisition requirements to mission outcomes defined as functions, capabilities, and service levels
- Refocusing operating funds to leverage newer acquisition models such as IT-as-a-service and cloud, which reduces waste and ensures that agencies deploy the exact technology they need, when and where they need it

The result will be a significantly more agile, innovative, and secure network infrastructure that enhances mission outcomes, promotes innovation, and reduces overall costs.

For more information, visit:

ruckusnetworks.com/products/service-assurance-business-intelligence

dell.com/networking