Federal agencies are discovering advanced wireless capabilities — and Network-as-a-Service strategies — can help augment and accelerate network modernization.
When the U.S. Department of Defense announced a series of Enterprise Infrastructure Solutions (EIS) task order awards worth nearly $1 billion last year for network modernization and technical support services, the task orders said as much about the changing nature of network infrastructure as they did about DOD’s push to modernize.

At the time, the task orders called for Verizon to transition the entire Pentagon military and civilian population from copper-based telephony to advanced internet protocol (IP)-based voice, video and data services. They also tasked Verizon to deliver core voice, transport, internet and related services to homeland security and defense professionals working in 370 locations throughout the National Capital Region.

Both initiatives reflected what federal IT officials had seen coming for many years: That software-directed, IP-based voice, video, and data were converging in ways that traditional networks were ill-equipped and largely outmoded to handle.

What agencies have underestimated, however, is how rapidly network infrastructure is evolving. The expanding capabilities of 5G, Multi-Access Edge Computing (MEC), Fixed Wireless Access (FWA) that uses 4G and 5G radio spectrum, small-cell Wi-Fi extension technology, low-latency satellite connections and higher capacity broadband capabilities are redefining the nature of network infrastructure. Collectively, those capabilities offer civilian and defense agencies a new generation of network versatility — and the ability to reimagine and rearchitect how they support their workforces around the globe.

Mounting strains on network infrastructure

Federal agencies have made monumental strides in modernizing parts of their IT operations. Defying skeptics, agency IT departments proved they could successfully migrate mission critical applications to the cloud while maintaining day-to-day operations during the pandemic. Agencies that did so are already experiencing the benefits of on-demand high-performance computing, deeper data analytics, faster detection and response to security threats and more scalable services to the public.

However, without also modernizing their underlying network services to leverage those cloud capabilities, agencies risk the prospects of maintaining the equivalent of a newly renovated office tower that kept the aging, sub-par wiring and plumbing in place behind the walls.

That not only prevents agencies from taking advantage of more agile networking and security capabilities but leaves them vulnerable to increasing strains on their networks, argues Brian Schromsky, Managing Partner, 5G Public Sector at Verizon. Chief among them, he says, are:

Growing pressures to handle data effectively.

The continuing escalation of data in transit places new demands on network performance. That includes intensive data collection about user behavior on agency networks, IoT monitoring, surveillance and threat detection tools. By deploying more modern, software-defined networks and analyzing data usage patterns, agencies can optimize their networks, predict bandwidth requirements, and tailor services to meet specific needs internally while significantly improving user satisfaction and response.

“It’s now possible to establish high-speed, secure and reliable connectivity with fixed wireless access without requiring cable or fiber to run underground [and is a] great choice for government agencies, as well as the private sector partners who help them build, operate, and maintain public infrastructure.”

– Brian Schromsky
Managing Partner, 5G Public Sector, Verizon
The need for ubiquitous and resilient connectivity.
Advances in wireless solutions are transcending traditional wired approaches. Fixed wireless access and private wireless networks offer alternatives to extensive cable infrastructure, reducing costs and complexities while ensuring reliable, more ubiquitous connectivity. Integrating 5G cellular and next-gen Wi-Fi technologies also provides agencies resilient backup options and continuity during terrestrial network outages, enhancing mission critical operations.

Support for a mobile and hybrid workforce.
The post-pandemic shift towards hybrid work models is forcing agencies to shift their IT investments from centralized office connections to remote and distributed setups, requiring robust connectivity and bandwidth but also greater flexibility to manage network resources as demands fluctuate.

Escalating risks of security breaches.
Network vulnerabilities continue to be one of the three primary ways attackers access an organization, according to the latest Verizon Data Breach Investigations Report. Modernizing network infrastructure remains a critical factor in addressing some of those vulnerabilities and meeting federal zero-trust implementation goals by 2024.

“All that said, I think one of the biggest challenges agencies need to focus on is understanding how and where people will be working moving forward,” said Schromsky.

“Agency leaders are starting to appreciate that their technology decisions — and how we use technology — will play a critical role in fostering a culture in the workplace. Technology isn’t just about making things more efficient and more secure. It’s also about empowering people to work more creatively and allowing citizens to interact with agencies more effectively.”

Rise of Network-as-a-Solution Services
It’s not that agencies don’t see the need for or the value of modernizing their network infrastructure. More often, “it's the challenges they face in moving from their modernization vision to the practical implementation of that vision,” said Schromsky.

Given the complexity of modernizing IT systems and the widening array of options, agencies are harder pressed than ever before to test and implement their preferred network solutions. They also face another hard truth: moving from vision to implementation requires more expertise and experience than many agencies possess.

Fortunately, just as agencies discovered the inherent advantages of adopting cloud-based services for their infrastructure, platforms and applications — including more immediate scalability, security and agility — agencies are recognizing those same advantages by adopting a Network-as-a-Service (NaaS) model.

NaaS solutions, like those available from Verizon, allow enterprises to adopt agile, automated network platforms consumed as a service. For agencies, that means moving from vision to implementation more quickly — and connecting users to applications and data across evolving cloud and work environments more reliably.

NaaS provides the means for “enabling the adaptive enterprise,” said Verizon’s Senior Vice President Global Enterprise, Massimo Peselli, in a recent white paper. Among other advantages, a NaaS approach gives agencies greater ability to:

Gain network visibility and control.
As agency requirements and their reliance on cloud services keep evolving, the need for SD-WAN to reconfigure network services quickly has become essential. But SD-WAN tools also give agencies greater visibility into the performance of the network and the applications running on it.

Adapt to AI/ML data growth.
The explosion of data and metadata requires advanced levels of automation and network function virtualization (NFV) to optimize performance. Turning over the mechanics of network management to a NaaS provider gives agency personnel greater bandwidth to focus on mission outcomes and less on configuration bottlenecks.

Shift to SASE faster.
Secure access service edge (SASE) is becoming the dominant model for how enterprises operate in a decentralized, mobile-first and cloud-first world. Adopting SASE architecture allows enterprises to deploy, manage
and scale infrastructure more effectively and securely. At the same time, it allows agencies to support on-premises and cloud-based applications without needing to have separate infrastructure.

**Enhance network security.**
Network and security have become intrinsically entwined. By shifting to a NaaS model, agencies also benefit from more frequently updated security controls and a deeper roster of network security specialists than most agencies can maintain on their own.

**Leveraging global network experience**

Those advantages are multiplied when working with Verizon, says Schromsky. He points to Verizon’s decades of global network management experience and its extensive arrangements with partners providing the latest networking and security solutions. Add to that the experience and knowledge Verizon’s security experts have gained in observing and responding to real-time security threats across the globe.

Schromsky insists, however, that advances in network technology are poised to give agencies a new kind of advantage by being able to augment and even leapfrog legacy networks rather than merely upgrade them.

“It’s now possible to establish high-speed, secure and reliable connectivity with fixed wireless access without requiring cable or fiber to run underground. Private networking is a great choice for government agencies, as well as the private sector partners who help them build, operate, and maintain public infrastructure because it provides high levels of security and reliability,” he said.

“If you look at airfields, at ports, at university campus environments, where you’re starting to handle all kinds of devices and video surveillance, you can start to deploy WiFi and fixed wireless access to complement, rather than rip and replace existing wired networks. Now you can build a private network that covers 20 square miles, with two cell sites and lots of Wi-Fi access points,” he explained.

“We understand the critical nature of the work we will do with the FBI to improve network availability, enhance operational efficiency, use tailored approaches to meet individual division needs, and help modernize technology.”

– Maggie Hallbach, Senior Vice President, Public Sector, Verizon

The ability to integrate advanced wireless capabilities with existing IT infrastructures was one of the reasons the FBI awarded Verizon Public Sector a $400 million task order last year, according to Maggie Hallbach, Senior Vice President, Public Sector at Verizon.

The project involves delivering ethernet access capabilities and resilient, global Virtual Private Network Services (VPNS) with a Verizon 4G LTE and 5G Nationwide cellular fixed wireless access arrangement. When completed, the FBI expects to benefit from high-speed connectivity for agents working in the field and greater continuity of services at key FBI locations.

While the task order was part of broader plans by FBI officials to overhaul its network, the award recognized Verizon’s network expertise as well as its familiarity with the unique requirements of federal agencies.

“We understand the critical nature of the work we will do with the FBI to improve network availability, enhance operational efficiency, use tailored approaches to meet individual division needs, and help modernize technology,” said Hallbach.

**Find out more how Verizon can help your agency transition to modern network serves.**

This report was produced by Scoop News Group, for FedScoop and underwritten by Verizon.