



Transition to transformation in federal IT



Federal-civilian agencies have dedicated substantial time and resources to the complex transition from the legacy Networkx contract to the government's Enterprise Infrastructure Solutions (EIS) vehicle. The magnitude of that effort often left little bandwidth for broader network transformation initiatives.

Now, with the EIS transition reaching completion in 2026, agencies are shifting focus from contract migration to modernization — upgrading network infrastructure, enhancing performance and security, and adopting the next generation of networking technologies needed to support mission demands.

"Federal agencies are behind the commercial environment by probably five to seven years in technology, and now it's time for a major network transformation," said Jason Tolbert, vice president of federal civilian at AT&T.

In practice, this transformation extends far beyond traditional network upgrades. Federal agencies are modernizing their technology environments to support a wide range of mission requirements, including cloud adoption, AI deployment, workforce collaboration, application modernization and enhanced citizen services.

Key initiatives include implementing software-defined wide-area networking (SD-WAN), adopting Zero Trust Network Access (ZTNA) architectures, migrating applications and workloads from data centers to the cloud, transforming legacy voice systems into unified communications and contact center platforms, and replacing aging copper infrastructure with fiber-based connectivity.

Agencies are also evaluating emerging access technologies such as Low Earth Orbit (LEO) satellite services and fixed wireless solutions to improve connectivity diversity, resilience, and cost efficiency. Strengthening cybersecurity remains a top priority objective, but it is one element of a broader effort to build more agile, scalable, and mission-ready network infrastructures.

"As mission requirements and cybersecurity challenges become more complex," Tolbert said, "the old methodologies just aren't going to cut it."

Critical software-defined steps for the future

“The old ways” include copper-based Time Division Multiplexing (TDM) infrastructure, which remains in use across portions of the federal government despite being ill-suited for today’s mission demands. The growth of cloud-based applications, AI-enabled services, real-time video collaboration and hybrid workforce models has dramatically increased network requirements, while modern security architectures demand greater agility and visibility. Legacy copper-based networks simply were not designed to support the performance, scalability, and resiliency these capabilities require.

Implementing SD-WAN is an important step in modernizing federal network infrastructure. Rather than relying on traditional static network architectures, SD-WAN enables agencies to intelligently orchestrate traffic across multiple transport types while prioritizing application performance based on mission needs.

This approach enhances network resiliency, improves visibility into application and network performance provides greater flexibility to optimize the cost and effectiveness of underlying connectivity services. It also establishes a more agile foundation for cloud adoption, AI-driven applications, and other emerging technologies.

Moreover, when agencies combine SD-WAN with converged fiber and wireless capabilities, they gain diverse connectivity paths to critical workloads. “That combination provides a significant resiliency advantage,” Tolbert said. “If one path is disrupted, traffic can be redirected to help maintain mission continuity.”

Modernizing security models

Agencies must reimagine what cybersecurity looks like in the modern world of decentralized work alongside modernizing the network. As employees travel between office, home and the field, a zero trust framework based on continuous authentication enables a more mobile workforce.

According to previous security models under early Trusted Internet Connections (TIC) recommendations, agencies followed a hub-and-spoke approach. All traffic had to be backhauled to a hub before moving to the final destination.

“Every single packet had to all come to a central location. If I was in the middle of the country and my data center was in Los Angeles, I had to send my packets all the way to Los Angeles, even if the data I needed was only a few miles away,” Tolbert said. “That’s very inefficient.”

TIC 3.0 supports a more flexible approach. By combining zero trust principles with cloud-delivered security capabilities such as Security Service Edge (SSE), agencies can provide users with secure, direct access to authorized applications and workloads — without requiring every connection to pass through a central hub.

“I no longer need to have everything centralized to one place. I connect directly to the things I need — I could be in the field, I could be at home, I could be at work, the device I need can connect securely wherever it is,” Tolbert said. “So I have a very mobile workforce using those digitized capabilities that could be right in my hand.”

For federal IT leaders, the outcome is not simply a more mobile workforce. It is a security architecture designed to reduce unnecessary network complexity, support cloud adoption and deliver consistent protection wherever the mission takes place.



The first responder network

The true test of network transformation is not just about daily efficiency but how it performs in a crisis. Whether a cyberattack or a natural disaster, agencies must have fast, reliable communications to support mission-critical operations.

“What is becoming increasingly more important, especially when responding to emergencies, is interoperability,” Tolbert said. “And no one really has the essence we can bring to bear for temporarily setting up network connectivity when it comes to our FirstNet network.”

The only nationwide network built specifically for first responders and the public safety community, FirstNet is highly secure and has the ability to prioritize, during disasters, critical first responder traffic. To further underscore AT&T’s commitment to the first responder and public safety communities, AT&T will be rolling out FirstNet Fusion.

“Fusion would be the first platform that provides universal interoperability capability in an open standard, which will allow all sorts of first responders on varying platforms to all talk together in a secure and convenient way,” Tolbert said. “We think this will really change the game around first responders.”



Creating a foundation for AI advancement

Much of the network modernization process is centered around preparing the federal-civilian workforce for increased AI, agentic automation and other data-heavy technologies to come. AI is fueled by data and bandwidth — and agencies need a lot of both.

“Maybe an agency was never really taking advantage of the power that was in the data sets that they have,” Tolbert said. “They’re going to have to rationalize those data structures, consolidate those data structures, and move that data around so that AI can understand that data ... give you great insights, and help you make decisions in your business, and that’s going to take very high capacity.”

Agencies cannot accommodate onsite the massive amounts of compute power required to fully leverage AI. Data must be able to move quickly and with low latency between geographically dispersed data centers and hyperscaler environments.

“You need to be able to connect to the hyperscalers, and you’ll want to work with a network provider that has those hyperscalers pulled onto their backbone,” Tolbert said. “You don’t want to be passing your traffic through multiple service providers to get to the hyperscaler.”

As the largest fiber and wireless network provider, Tolbert added, hyperscalers are connecting directly into AT&T’s backbone, creating a seamless path for agencies to their massive data sets.

A mission-first partner for network transformation

Federal-civilian agencies are navigating a pivotal time in technology, but they don’t have to do it alone. Shifting from legacy hardware to an agile, software-defined network future is a daunting, complex prospect. Agencies can tap industry partners like AT&T for specialized migration expertise and professional services support.

“AT&T has the largest contingent of government professional services than any other carrier. We have more cleared resources than any other carrier, do more business in the high-security national security space than any other provider,” Tolbert said, “and with that we have the people and the expertise to actually help agencies do the work.”

As federal IT leaders shift from the logistics of EIS transition to transformation, they have the opportunity to rethink network architecture, remodel their cybersecurity approach and build a resilient, high-capacity foundation to support next-generation technologies.

“Our solution mindset is around mission first,” Tolbert said. “How do we deliver the solution that enables that mission and enables better total cost of ownership, increased productivity for the agency, and more resiliency and redundancy? That’s what we really bring to bear as we help civilian agencies through network transformation.”

Learn more about how AT&T can support federal-civilian agencies on their modernization journeys.

Learn more