Empowering Today's Government:

The Role of Private Connectivity Fabric in Achieving Agility and Resilience

LUMEN

Microsoft

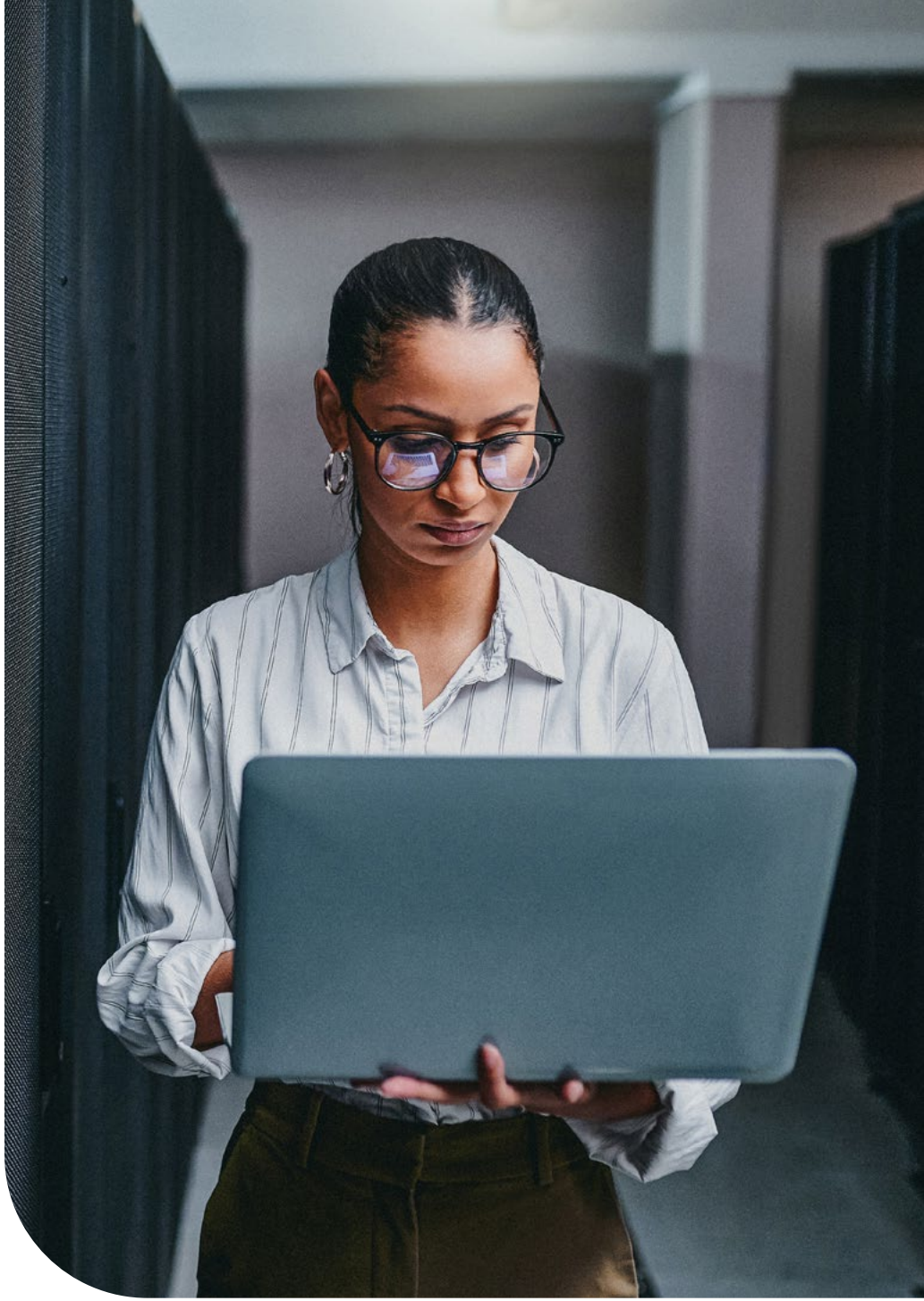
Contents

Introduction

Change is a certainty in the federal government, from cyber threats by nation-states to the needs of U.S. citizens. In response, federal CIOs are being asked to show greater agility and resilience as the workforce is restructured, the need to adopt AI grows, and legacy systems continue to age and require updating to meet the needs of tomorrow. To help address these challenges, modernized, resilient networks are urgently required—to ensure uninterrupted communication and information flow, and to support an effective data strategy in an increasingly data-driven era.

The federal government is restructuring to meet the demands of a new administration and a range of new requirements. Amidst these changes, the intelligence community, Department of Defense, and federal civilian agencies need effective strategies to ensure the security and integrity of data. And every data strategy in turn needs a network strategy in order to effectively support the mission.

To keep up with growing data demands, the network needs to be flexible, agile, and secure. Agencies need low-latency, high-bandwidth connectivity and built-in security to ensure that data can traverse the network and deliver data-driven insights at the point of need. This becomes increasingly important in today's cloud and AI-driven environments.



Challenges: A changing landscape demands a new approach

A number of current challenges highlight the importance of a modernized approach to networking in government. Gartner for instance identifies the need to address:

- **Workforce realignment:** Under the "Return to Work" Executive Order, thousands of federal workers are returning to the office. Yet many government facilities lack the modern, hardened network equipment needed to support a massive return to on-site work.

- **Cost concerns:** The demands for always-on data from edge, core, and cloud requires advanced connectivity, but upgrading and maintaining highly secure networks is expensive, requiring investments in things like diverse fiber routes, backup power, specialized hardware, and personnel.

  The Information Systems Audit and Control Association (ISACA) points to costs associated with wages for maintaining in-house network engineers, hardware repair and maintenance costs, and also to indirect costs "such as research and development, expenses associated with employee recruitment and training costs"—all of which can pose barriers to upgrades.

- **Security concerns in legacy systems:** Government networks are constant targets for cyberattacks from hostile actors, both nation-state adversaries and criminal organizations. Maintaining effective security is an ongoing challenge.

  "Nation-states are some of the most sophisticated actors that conduct cyberattacks," the Congressional Research Service reports, and they are known to target federal systems. In December 2024, for example, Chinese hackers breached the U.S. Treasury Department, gaining access to over 3,000 unclassified files, according to the Center for Strategic and International Studies.

- **Advancing Artificial Intelligence:** The growing use of AI and automation in government systems have been shown to put added strain on existing network capacity. "On average, answering one chat request typically uses around 1-2 KB if only the final output text is weighed up. However, that doesn't tell the whole story. Behind-the-scenes there's extensive data usage during training phases," Data Science Central reports.

  "Modern AI use cases, such as autonomous systems, large-scale language models, predictive analytics, and real-time image or video processing, require robust infrastructure supporting high-speed data transfers between distributed data centers, edge devices, and cloud platforms," according to analysts at Frost & Sullivan.

  As agencies adopt AI-enabled applications, all this puts a strain on network capacity and may exceed the capabilities of present networks. The Defense Department for example employs over 676,000 civilian workers. As personnel are encouraged to use GenAI tools, it's easy to see how adoption on that scale would strain existing network capabilities.

- **Specific challenges in network modernization**
  In Intel and Defense: Time is a major factor for these organizations, as modernizing networks is a labor-intensive process with a limited pool of vendors and suppliers approved for government use. Delays increase risks.

  Supply chain issues compound the problem. "Disruption in the supply chain remains the top-of-mind challenge for many" and can interfere with the timing around modernization efforts, Frost & Sullivan reports. They note that delays in network equipment supply, including switches, routers, and fiber, can directly impact a network upgrade and expansion plan.

  In Federal Civilian: Investing in upgrading existing infrastructure to support remote work and daily operations is a key challenge.

Back-to-office requirements are straining capacity, and the data demands associated with rising AI usage adds urgency here.

"AI in general is the wild card in the deck. The mysterious future directions for this technology suggest that AI broadband and wireless bandwidth needs could conceivably exceed 1 Gb/s," IEEE reports.

As multiple mission centers and program offices develop AI capabilities, it is crucial to build a robust, scalable AI infrastructure that supports organizational growth."

— GSA: AI Guide for Government

The solution: A private connectivity fabric

An approach to networking known as a private connectivity fabric offers a way forward for federal agencies looking to modernize their networks in support of an effective data strategy. For CIOs looking to improve efficiencies, prepare for return-to-office, and accelerate AI initiatives, this approach delivers the flexibility, agility, and security needed to meet today's growing data demands. With low-latency, high-bandwidth connectivity, and built-in security, a private connectivity fabric delivers the modernized, resilient capability needed in today's cloud and AI-driven environments. Private connectivity fabric refers to a customized architecture, one that is designed to give organizations control over their sensitive data. As a highly customized, secure network infrastructure, a private connectivity fabric offers features such as redundancy, scalability, and managed services, with high levels of protection, encryption and access control and authentication. It also includes visibility into the network for optimization and troubleshooting.

Advanced connectivity spans across data clouds, hyperscalers (AWS, Google Cloud, Microsoft, etc.), as well as data centers and SaaS clouds. All this helps to keep up with data that is in flux and growing exponentially as workloads of the future continue to evolve and expand.

Public-sector agencies rely on public cloud providers, and those providers in turn are leaning into private connectivity fabric. Microsoft for example turned to Lumen for "a custom network that includes dedicated access to existing fiber in the Lumen network, the installation of new fiber on existing and new routes, and the use of Lumen's new digital services," IEEE reports. "This AI-ready infrastructure will strengthen the connectivity capabilities between Microsoft's datacenters by providing the network capacity, performance, stability and speed that customers need as data demands increase."

Beyond addressing the data demands, this approach supports risk mitigation. Private network fabrics are built for a targeted purpose, with specific performance, access, and security in mind. This approach to networking "mitigates potential risks and protects critical infrastructure.

Higher security requirements are achieved by dedicated security credentials. Individual agency security needs depend on their risk tolerance," according to experts in an Advanced Technology Academic Research Center (ATARC) working group. The working group notes that this strategy brings to bear "dedicated resources that improve performance, security, privacy, and safety."

Private connectivity fabric has the potential to deliver in ways that commercial networks cannot, and DoD sees potential benefit here. Its 5G strategy recognizes that "under certain circumstances, commercial 5G may not fulfill DoD's requirements." It notes that private networks could help to close the gap, supporting an infrastructure that enables warfighters "to ingest and transfer massive amounts of data—a capability that will be critical for the U.S. to retain information and decision advantage."

Partnerships to Support Government Missions

Public-private partnerships are crucial for the federal government, offering myriad benefits that enhance national security, technological advancement, and economic growth. These collaborations foster information sharing and cooperative action, which are essential for protecting critical infrastructure and advancing cybersecurity.

For instance, partnerships between Lumen and major tech companies like Microsoft have demonstrated the power of combining private sector innovation with public sector needs. These alliances enable the federal government to leverage cutting-edge technologies and secure, scalable network infrastructures that are vital for the AI-driven future. By working together, tech firms and government agencies can improve national technologies and security systems, ensuring a robust defense against cyber threats while also driving digital transformation.

How does this address the current challenges?

A private connectivity fabric offers inherent scalability, security, flexibility, and other key features that help federal agencies to address their most pressing challenges.

Private networks may augment or supplement commercial services because they are tailored to each installation's mission needs, security, and military-unique capabilities."

— U.S. DoD

- **Scalability:** Tailored to meet an agency's specific needs, a private connectivity fabric can deliver scalable bandwidth. This aligns with DoD's efforts to "invest in IT infrastructure that is agile and scalable, capable of adapting to ever changing business requirements and mission demands.

- **Resilience:** This approach can help agencies to meet the urgent need for more robust security and resilience. ATARC experts point to the ability of private networks to deliver enhanced security through the use of dedicated security credentials.

- **Flexibility:** Being highly customizable, a private connectivity fabric delivers flexibility as mission needs evolve. "As enterprises run AI workloads on the cloud and their business requirements become increasingly complex, they will need intelligent network services that give them more flexibility and control," McKinsey reports.

- **AI Demands:** The industry trade organization 5G Americas says that AI will demand networking solutions that help "to unlock transformative opportunities." A private connectivity fabric provides the high-speed, low-latency connections needed to enable and scale AI applications across government networks.

Isolation from public networks [enables] dedicated resources that improve performance, security, privacy, and safety."

— ATARC

Use cases for hyperscalers, data centers, and enterprise

Agencies can look to tap the power of this approach via their hyperscaler relationships; between their data centers; and across the organization.

- **Hyperscalers** require "ultra-low latency and high bandwidth as well as real-time access" so that information can be leveraged for use by applications, ETSI reports. Private networks enable global low-latency connectivity to cloud services, and government agencies can leverage their existing relationships with hyperscalers to tap that potential.

- **Data centers:** Government needs high-speed, scalable connectivity between data centers. The Energy Department for example has called for a push to "accelerate data center interconnection" and private networks can help to meet that need.

- **Enterprise:** GSA emphasizes the need for "seamless, secure operating environments through customized telecommunications services." A private connectivity fabric offers a way forward, with secure, high-bandwidth connectivity tailored to user needs.

Role of managed services

Managed services support government efforts to elevate efficiency and cost-effectiveness, allowing agencies to offload the day-to-day operations and maintenance of their private network infrastructure.

ISACA notes that "managing enterprise networks to meet increasing business requirements in the face of consistent cost reduction pressures can be demanding." They go on to say that managed service providers can help here "because they employ a wide range of highly trained and experienced engineers who are specialists in network security, enterprise architecture, switching and routing and other technical areas, leading to greater reliability, availability and resiliency."

Network managed service providers (NMSPs) have the potential to deliver all-inclusive and truly exceptional high-quality services."

— ISACA

Achieving a private connectivity fabric

For planning purposes, it's important to know that private connectivity requires access to fiber optic networks, either through existing infrastructure or new fiber installations. Extensive permitting processes and coordination with various authorities can add time and complexity.

"Managing the zoning, planning and permitting process, construction, turn up, test and optimization" all present potential complications, NTIA notes. Implementation management services can help guide agencies here.

Agencies can also look to draw support for this effort from their commercial cloud providers. As they look to integrate private connectivity, government agencies already leveraging cloud services like Azure and AWS can build on those relationships to help them extend their network reach and capabilities.

Strategic advice

Agencies looking to improve their networking capabilities can leverage the GSA's Enterprise Infrastructure Solutions (EIS) contract and other contracting vehicles to streamline acquisitions. And they can take concrete steps today to get the ball rolling:

- Understand your current data strategy. Where does your data sit (on-prem, cloud, multi-cloud) and how do you transport, store, and secure it?
- Examine existing or new use cases for multi-cloud or AI. What level of bandwidth and security does it require? Do you have a network strategy to support these efforts?
- Act quickly, as delays increase security risks and costs.
- Engage with industry partners that are already investing and expanding in the infrastructure that you need.

Message from our sponsor

Many organizations today are racing towards AI readiness and often overlooking the network's impact on their goals. With a long history in helping agencies accelerate transformation and enable process, **Lumen is the trusted network for AI.** We digitally connect people, data, and applications to quickly and securely enable the mission. Our depth of network visibility and integration translates into improved situational awareness that elevates your agility, threat response, and decision confidence.

A New Way of Networking: Lumen® Private Connectivity Fabric℠ enhances agency agility by providing network resilience that withstands increasing data volumes that often are associated with AI. The vast Lumen network is built to power AI initiatives. Lumen expects to end 2025 with 16.6M intercity fiber miles and for that total to increase to 47M intercity fiber miles by the end of 2028. These custom network architectures are designed to provide high-speed, secure connectivity that supports AI and real-time decision making.

The Payoff: Lumen PCF enables an AI-ready infrastructure with -25% optical loss vs. wider market, ≤5ms of latency at the edge, designed to cover up to 97% of U.S. business demand, and 60% more capacity vs. legacy fiber. (Note: ~25% less fiber optic loss per km; less loss translates to less frequent need for fiber optic signal regeneration, decreasing equipment costs; figure is based on a comparison to vintage 2000 fiber [decrease from .22 db/km loss to.17 db/km].)

About

Lumen

Lumen is a global communications services provider that ignites business growth by connecting people, data and apps—quickly, securely and effortlessly. Our networking, edge cloud, collaboration and cybersecurity solutions and managed servicesbare designed to elevate your business and deliver the most user friendly, intuitive and productive technology environments.

Visit Lumen.com and learn more about the company and the trusted network for AI.

GBC

Government Business Council (GBC), a portfolio platform of GovExec, is dedicated to advancing the business of government through analysis, insight, and analytical independence. GBC studies industry research reports and insights from influential decision makers from across government to produce intelligence-based analysis of industry trends. Learn more at govexec.com/insights.

Microsoft

Microsoft (Nasdaq “MSFT” @microsoft) creates platforms and tools powered by AI to deliver innovative solutions that meet the evolving needs of our customers. The technology company is committed to making AI available broadly and doing so responsibly, with a mission to empower every person and every organization on the planet to achieve more.

Visit Microsoft.com to learn more.


LUMEN
Microsoft