GovCIO MEDIA & RESEARCH

APRIL 2026

DeepDives

IT Modernization Driving AI EFFICIENCY

SPONSORED BY

LUMEN® | cisco Partner

INSIDE:

Table of Contents

Bridging the Federal IT Modernization Gap

Federal agencies face urgency to modernize legacy environments for new working realities.

The United States federal government stands at a critical juncture in its technological history. Faced with an environment defined by escalating nation-state cyber threats and the transformative potential of artificial intelligence, the modernization of federal IT is not optional, but rather a foundational requirement for national security.

A significant barrier to modernization remains: the massive “technical debt” accumulated over decades. Approximately 80% of the federal IT budget, which exceeds $100 billion annually, is currently dedicated to maintaining obsolete and often insecure legacy systems. This leaves only $20 billion for the innovation required to lead in the AI era. For federal technology leaders, bridging this gap is the defining challenge of 2026.

The High Cost of Stagnation: Technical Debt as a Security Risk

Technical debt is more than a budgetary burden; it is an expanding attack surface. Every dollar spent on unpatchable legacy systems is a dollar diverted from the zero trust protections mandated by the White House. Industry assessments suggest that up to 30% of enterprise network assets are unknown or undocumented at any given time, creating dangerous security blind spots. Without an accurate, real-time inventory, agencies cannot effectively secure or modernize their infrastructure.

Legacy “spaghetti” architectures, characterized by on-premises, perimeter-based defenses, are fundamentally inadequate for the modern mission. The transition to a zero trust security model, where no user or device is automatically trusted, is essential. Modernization requires a shift to identity-centric environments where access is continually verified based on context and risk. (ctd.)

Photo credit: Shutterstock AI Generator

The Physics of AI: Infrastructure Must Precede Deployment

A common pitfall in federal AI strategies is the assumption that AI is purely a software layer. In reality, the "physics" of AI workloads — specifically their immense bandwidth and low-latency requirements — will overwhelm legacy networks. AI broadband and wireless needs are projected to conceivably exceed 1 GB/s.

To support these demands, the physical layer must evolve. This will require innovative solutions like Lumen® Connectivity Fabric™, a modular architecture that combines wavelengths, dark fiber and colocation. This will require an AI infrastructure fabric approach that enables private connectivity through dark fiber, colocation and high-capacity wavelengths. Lumen's AI-ready infrastructure allows for approximately two times more fiber within existing conduits, resulting in a 60% increase of capacity compared to legacy networks allow. For agencies, this equates to a high bandwidth, low-latency backbone that can handle terabytes of data that move at speeds needed for AI intensity.

The Human Factor: Closing the AI Skills Gap

Modernizing technology is futile without aligning human resources. The federal government faces a persistent challenge in recruiting and retaining data scientists and AI specialists against private-sector competition. The solution to this problem lies in the adoption of network-as-a-service (NaaS) and AI-as-a-service (AIaaS) models.

NaaS allows agencies to operate networks without the burden of maintaining underlying hardware. By utilizing a "single pane of glass" for visibility across the entire enterprise, network engineers are freed from routine maintenance to focus on real-time troubleshooting and mission-critical outcomes. This "augmentation" of human talent allows federal engineers to become better network engineers by focusing on higher-value tasks like anomaly detection and predictive self-healing. (ctd.)

Photo Credit:
Shutterstock AI

Procurement Agility: From ‘Buying Boxes’ to ‘Buying Outcomes’

Technical agility is impossible without procurement agility. The traditional government-owned, contractor-operated (GOCO) model often results in multi-year delays through capital budget cycles. Shifting to a contractor-owned, contractor-operated (COCO) model allows agencies to leverage infrastructure-as-a-service and capital-as-a-service.

A prominent case study involving a law enforcement agency transition illustrates the value. By utilizing a COCO model, the agency saved $30 million in up-front capital costs and realized $8 million in operating expense savings over the life of the contract. Modern procurement vehicles like the $50 billion Enterprise Infrastructure Solutions (EIS) contract facilitate this transition, allowing agencies to move away from terrestrial telecommunications toward agile, cloud-based solutions like SD-WAN.

Conclusion: The Strategic Path Forward

As federal agencies look toward 2030, mission success will be measured by the ability to rapidly adopt and secure groundbreaking technologies. The roadmap involves three critical actions:

- Eliminate Technical Debt: Move beyond static tracking (like Excel) to real-time, data-driven network intelligence.
- Build AI-Ready Foundations: Prioritize private connectivity fabrics to ensure the internet of yesterday does not throttle the mission of tomorrow.
- Embrace As-a-Service Models: Utilize NaaS and AIaaS to bypass capital outlay hurdles and realign the workforce with mission-critical innovation.

By fundamentally re-architecting how the government interacts with its data and infrastructure, agencies can build a resilient digital enterprise capable of meeting the challenges of a competitive and dangerous digital landscape.

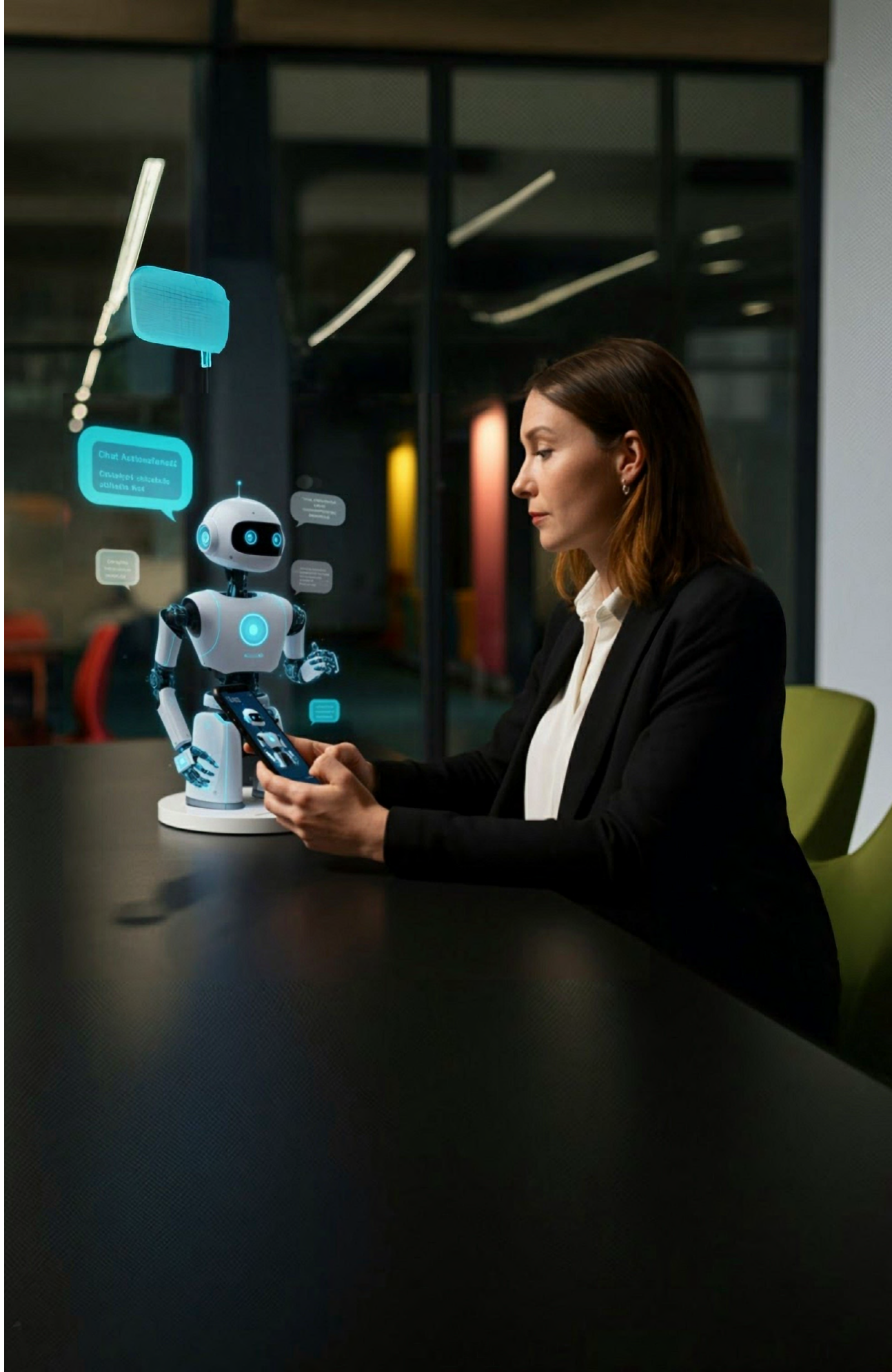

Photo Credit:
Shutterstock AI

GovCIO MEDIA & RESEARCH

LUMEN® | CISCO Partner

Inside the Push for AI-Ready Infrastructure

Mike Witzman
Vice President,
U.S. Public Sector Engineering,
Cisco Systems

Campbell Palmer
Vice President,
Technology Solutions Support,
Lumen Public Sector

Experts discuss what's holding agencies back from AI adoption and how to build a secure, scalable foundation.

What are the biggest challenges you're seeing around security, legacy infrastructure and operational complexity as agencies look to modernize IT environments to support AI?

Witzman Current AI adoption is largely focused on general productivity around discrete mission capabilities. That is surging right now. That's mostly being delivered today by industry and mission partners as a service, which brings a couple challenges for CIOs. First is mission as capability overhang. That is where AI capabilities are coming faster than we're prepared to absorb and adopt them. Due to cost predictability and cybersecurity concerns, we're seeing agencies prefer to build production AI

capabilities on-prem into the data centers that we've been evacuating for the last 10 years. The issue is those facilities weren't designed to handle the power and cooling demands required for full-scale AI systems.

Palmer Agencies need to have a real understanding of where their AI capability foundation resides, including where they want to do their LLM modeling and their data lake. Capacity is key. Agencies must validate that data centers have not just fiber access, but advanced, ultra-low-loss fiber capable of supporting multi-terabyte throughput on a single dark fiber strand. Users are going to be spread throughout the entire world. While the LLM may be fully functioning, operational and integrating within the data lake environment that it supports, enabling the users to reach into that LLM from anywhere is critical.

What role does a trusted infrastructure foundation play in helping agencies move from experimentation to real AI-driven outcomes?

Witzman Networks will play a central role in protecting AI agents and systems from tampering or compromise. Managing security policy across a highly distributed environment is critical, and we're addressing that through concepts like a hybrid mesh firewall.

Palmer Agencies must implement a layered set of controls to secure data and ensure its relevance. Agencies not only need to know where that data resides, but also who should have access to that data. Identity and access controls must be put in place through the appropriate systems, whether it's something as simple as role-based access control (RBAC) or some other mechanism to control who has access. (ctd.)

"Capacity is key. Agencies must validate that data centers have not just fiber access, but advanced, ultra-low-loss fiber capable of supporting multi-terabyte throughput on a single dark fiber strand."

—Campbell Palmer, Vice President, Technology Solutions Support, Lumen Public Sector

What should agencies be prioritizing now to be AI-ready, not just AI-curious?

Palmer Agencies need to define their use cases and understand the capacity requirements within their data center environments. They must design their networks to support that scale, including handling terabytes of data per second moving between facilities. They should prioritize getting that information and data as close to the end users as possible in a scalable framework.

Witzman The sheer scope of the opportunity that AI presents, and the need for it, means that CIOs are uniquely responsible for ensuring that the right culture within their organization is in place to balance opportunities and challenges that will come with it to keep the organization moving forward.

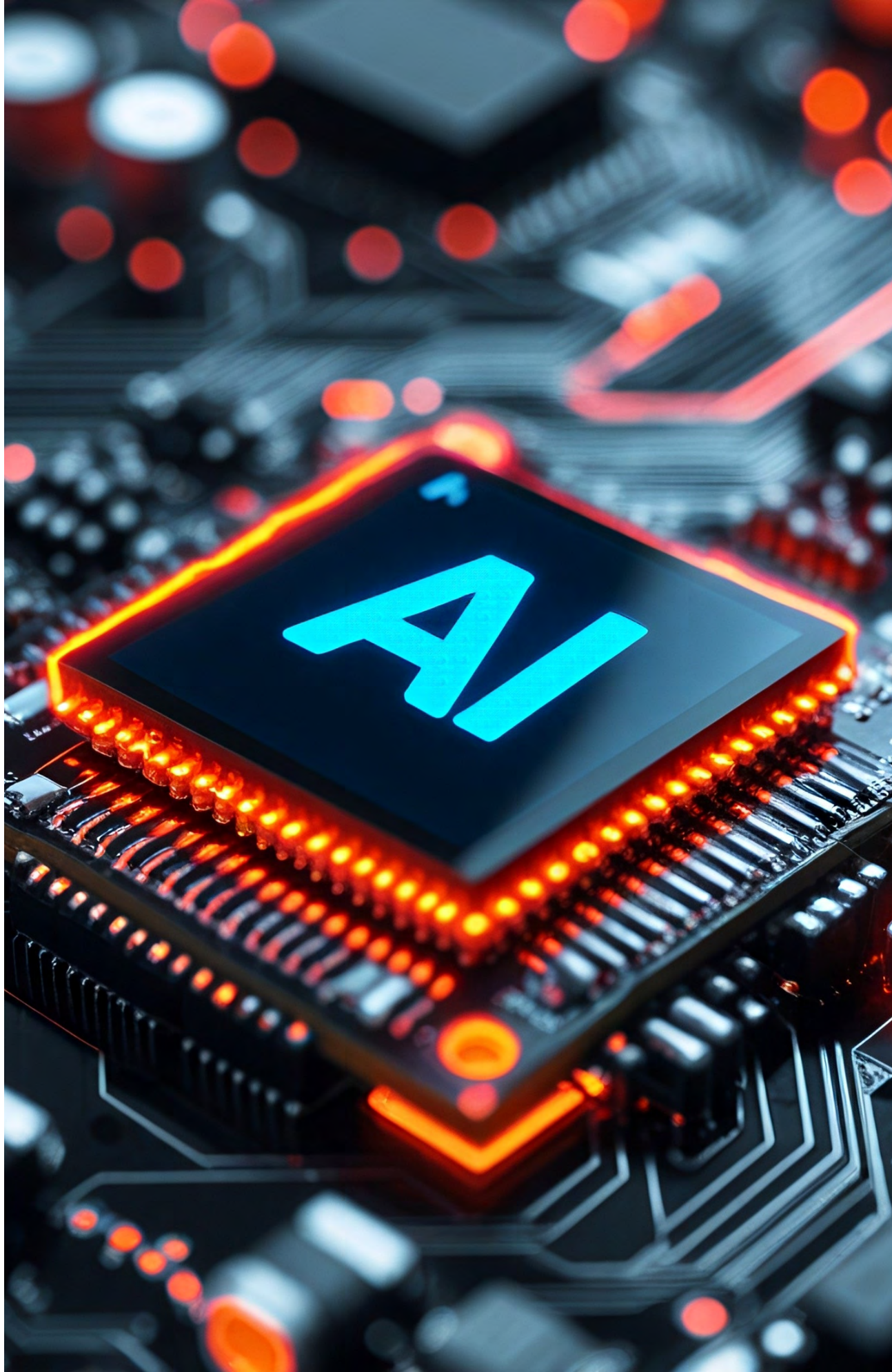

Photo Credit: DVC Designer/ Shutterstock

LUMEN®

Network modernization that delivers when public services can't wait

Networking | Edge Cloud
Cybersecurity | Collaboration
Managed & Professional Services

Lumen.com/public-sector

AI-Enabled Enterprises Turn Attention to Connectivity Fabric, Intelligence Use Cases

Expanding attack surfaces from increasingly digital environments require AI to keep up with continuous threats.

The integration of AI has shifted from a visionary goal to a foundational requirement for national security and operational continuity. For federal CIOs, CTOs and chief AI officers, the challenge is no longer just about buying AI, but also architecting an environment where data, security and mission-critical applications can leverage machine learning at scale and at the edge.

The transition toward a modernized environment is not merely a technical upgrade, but a strategic investment in the long-term health of the nation's digital infrastructure. By prioritizing the replacement of outdated equipment and enforcing rigorous lifecycle management, the federal government can unlock the potential of emerging technologies like AI while simultaneously reducing its attack surface.

To successfully build this intelligent environment, federal leaders must focus on several core operational and strategic pillars:

Proactive, AI-Driven Security

The traditional "castle-and-moat" security model is obsolete in today's landscape of distributed cloud resources and rapid nation-state threats. Architecting an AI-ready environment requires zero trust architecture augmented by machine learning. By integrating AI into the network fabric — using platforms like Lumen's Black Lotus Labs or Cisco's Talos — agencies can proactively analyze billions of signals in real time. This allows them to detect hidden anomalies like lateral network movement or credential misuse before they are exploited. This approach creates "predictive resilience," using AI to harden systems while maintaining mission uptime and compliance with FISMA and CMMC 2.0.

(ctd.)

Photo Credit: Digineer Station/Shutterstock

Mission Enablement and the Private Connectivity Fabric

Within defense and intelligence operations, AI acts as a critical force multiplier for managing the modern data surge. AI-powered analytics can rapidly process massive, unstructured datasets such as signals intelligence, open-source data and satellite imagery, empowering the Intelligence Community to transition from reactive reporting to generating anticipatory intelligence. For the War Department, AI directly supports military readiness by facilitating predictive maintenance, automated logistics and real-time situational awareness for the warfighter.

To deliver these capabilities seamlessly from the combat cloud to the tactical edge, agencies must deploy AI-ready infrastructure that enables ultra-low latency and high-bandwidth capacity at speeds needed for real-time processing. Building this fabric requires:

- **High-performance networking and edge compute nodes.** These are essential for handling massive data throughput at the tactical edge.
- **Dedicated, secure bandwidth.** This is private bandwidth that bypasses public internet backhaul to help ensure that sensitive AI workloads can operate securely and without delay, even in contested environments.

A private connectivity fabric is an AI-ready architecutre that combines dark fiber, conduit and colocation to create a private network that gives organizations absolute control over their data. This architecture is particularly relevant for DOW, whose 5G strategy recognizes that commercial networks may not always fulfill the stringent requirements for mission-critical operations.

Enhancing the Citizen Experience with High-Impact Use Cases

Beyond the battlefield, AI is redefining how the government serves its citizens by advancing digital inclusion. Agencies can transition from broad mandates to a successful pilot-to-production pipeline by focusing on specific high-impact, low-risk use cases. (ctd.)

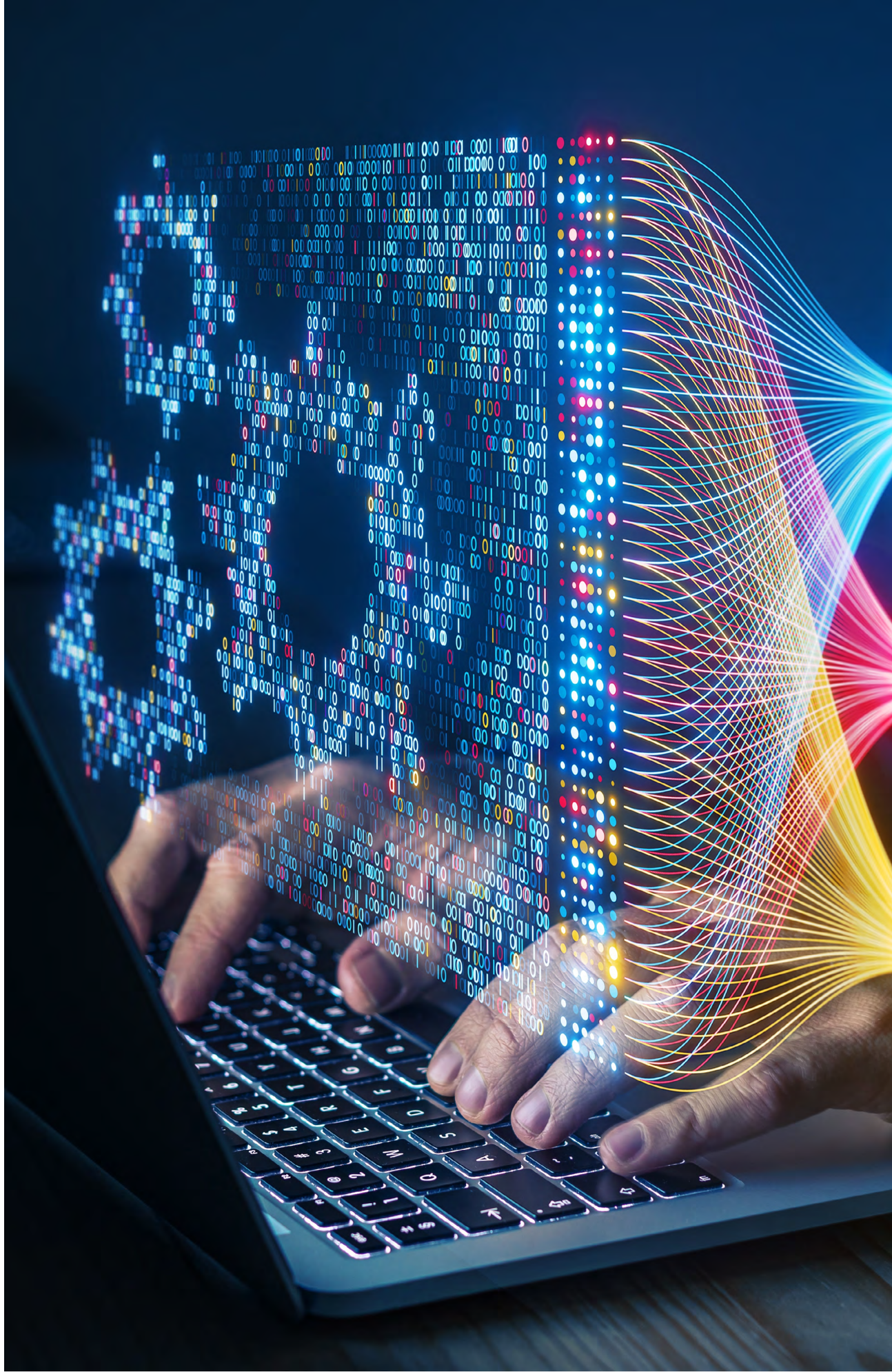

Photo Credit: NicoElNino/ Shutterstock

Practical applications include:

- **Automated document classification** leveraging AI to rapidly organize and categorize massive amounts of unstructured data.
- **Automated benefits applications** that streamline services to drastically reduce wait times and administrative burdens.
- **Intelligent chatbots** to efficiently handle routine but complex workflows, such as procurement queries.

By offloading these routine workloads to the AI engine to process in the background, federal programs can restore public trust and free up human personnel to focus on high-touch, high-value tasks that require empathy and nuanced judgment.

The Strategic Roadmap to Execution

Moving AI from hype to hands-on impact requires robust foundational capabilities. Federal leaders must prioritize:

- Data Management: AI relies entirely on the data feeding it. Agencies must implement a unified data strategy that breaks down silos, enforces robust governance and ensures data integrity.
- Infrastructure Readiness: Federal IT leaders must invest in the networking and compute infrastructure needed to handle massive AI data throughput.
- Specific Use Case Development: Leaders should target low-risk pilots to demonstrate clear value and build momentum before moving them to production.

The window for exploratory AI pilots is closing rapidly. Federal leadership must aggressively execute specific use cases and mature their data practices to build an enterprise that is genuinely intelligent — capable of sensing, responding and adapting to mission needs in real time.

Photo Credit: A9 Studio/ Shutterstock

GovCIO MEDIA & RESEARCH

DeepDives

Path to AI Modernization

STRATEGIC PILLARS:

1 PROACTIVE, AI-DRIVEN SECURITY

Architecting an AI-ready environment requires zero trust architecture augmented by machine learning. This approach creates "predictive resilience," using AI to harden systems.

SOLUTIONS: LUMEN BLACK LOTUS LABS, CISCO'S TALOS

2 MISSION ENABLEMENT AND PRIVATE CONNECTIVITY FABRICS

AI-powered analytics can rapidly process massive, unstructured datasets such as signals intelligence, open-source data and satellite imagery.

SOLUTION: PRIVATE CONNECTIVITY FABRIC, HIGH-PERFORMANCE NETWORKING AND EDGE COMPUTE NODES, DEDICATED AND SECURE BANDWIDTH.

3 ENHANCING THE CITIZEN EXPERIENCE WITH HIGH-IMPACT USE CASES

Agencies can transition from broad mandates to a successful pilot-to-production pipeline by focusing on specific high-impact, low-risk use cases.

APPLICATIONS: AUTOMATED DOCUMENT CLASSIFICATION, AUTOMATED BENEFITS APPLICATIONS, INTELLIGENT CHATBOTS